

T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ



**BAĞIMSIZ DENETÇİLERİN BİLGİ SİSTEMLERİ
DENETİMİNİN BAĞIMSIZ DENETİME ETKİSİ
KONUSUNDAKİ GÖRÜŞLERİ VE E-BELGE ÖZEL
ENTEGRATÖRLERİ BİLGİ SİSTEM DENETİMİNE İLİŞKİN
BİLGİ DÜZEYLERİNİN ARAŞTIRILMASI:
ANKARA İLİ UYGULAMASI**

DOKTORA TEZİ

DANIŞMAN
Doç. Dr. Ahmet Fethi DURMUŞ

HAZIRLAYAN
Zeliha KOCA

MALATYA – 2023

T.C.
İNÖNÜ ÜNİVERSİTESİ
SOSYAL BİLİMLERİ ENSTİTÜSÜ

BAĞIMSIZ DENETÇİLERİN BİLGİ SİSTEMLERİ DENETİMİNİN BAĞIMSIZ
DENETİME ETKİSİ KONUSUNDAKİ GÖRÜŞLERİ VE E-BELGE ÖZEL
ENTEGRATÖRLERİ BİLGİ SİSTEM DENETİMİNE İLİŞKİN BİLGİ
DÜZEYLERİNİN ARAŞTIRILMASI: ANKARA İLİ UYGULAMASI

DOKTORA TEZİ

HAZIRLAYAN
ZELİHA KOCA

DANIŞMAN
DOÇ. DR. AHMET FETHİ DURMUŞ

MALATYA-2023

ONUR SÖZÜ

Doç. Dr. Ahmet Fethi DURMUŞ danışmanlığında hazırladığım “**Bağımsız Denetçilerin Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi Konusundaki Görüşleri ve E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeylerinin Araştırılması: Ankara İli Uygulaması**” başlıklı doktora tez çalışmasının bilimsel ahlak ve geleneklere aykırı düşecek bir yardıma başvurmaksızın tarafımdan yazıldığını ve yararlandığım bütün kaynakların hem metin içinde hem de kaynakçada kaynak gösterme yöntemlerine uygun şekilde referans göstererek yazıldığını onurumla doğrularım.

Zeliha KOCA

ÖN SÖZ

Tez çalışmamın her anında bilgi ve tecrübeleriyle beni sürekli yönlendiren, pandemi sürecinde yaşanan tüm olumsuzluklar ve sonrasında yaşanan 6 Şubat depremine rağmen sabrı ve hoşgörüsü ile sürekli yanımda olan tez danışmanım Doç.Dr. Ahmet Fethi Durmuş hocama teşekkürü bir borç bilirim.

Görüş ve önerileriyle, tecrübesinden faydalandığım gerek akademik hayatımda gerekse tez çalışmamda bana yol gösteren Prof. Dr. Yusuf Cahit Çukacı hocama, tez izleme komitesi üyesi Dr. Öğr. Üyesi Muzaffer Demirbaş hocama, tezimin uygulama aşamasında desteklerini esirgemeyen S.M.M.M. Selçuk Gülten beye, bilgi sistemleri baş denetçileri Mustafa Abdurrahman Büküm beye, Mustafa Kemal Parmaksız beye, Kolaysoft teknoloji A.Ş genel müdürü Kezban Boztürk hanımefendiye, Okan Köylü beye teşekkür ederim.

Doktora ders döneminden tezin sonuçlandırılmasına kadar olan süreçte birlikte yol aldığımız ve kimi zaman heyecanımı kimi zaman kaygılarımı paylaştığım teyzem S.M.M.M Selma Erol ve kardeşim Ramazan Aydemir'e teşekkür ederim. Her zaman yanımda olduklarını hissettiğim değerli anneme, babama ve kardeşlerime teşekkür ederim.

Teşekkürlerin en büyüğünü ise her zaman yanımda olan ve yaptığı büyük fedakârlıkla çalışma sürecimi sevgi, sabır, inanç ve hoşgörüsüyle destekleyen, varlığıyla bana güç veren sevgili eşim Tarkan Koca'ya, kızlarım Gökçe ve Tuğçe'ye etmek istiyorum.

**BAĞIMSIZ DENETÇİLERİN BİLGİ SİSTEMLERİ DENETİMİNİN BAĞIMSIZ
DENETİME ETKİSİ KONUSUNDAKİ GÖRÜŞLERİ VE E-BELGE ÖZEL
ENTEGRATÖRLERİ BİLGİ SİSTEM DENETİMİNE İLİŞKİN BİLGİ
DÜZEYLERİNİN ARAŞTIRILMASI: ANKARA İLİ UYGULAMASI**

ÖZET

Globalleşen dünyada işletmelerin artan rekabet nedeniyle başarı sağlayabilmeleri için teknolojideki gelişmelere bağlı olarak ortaya çıkan olanakları takip etmeleri ve kullanmaları gerekir. İşletmelerin birleşmesi, büyümesi ve büyüyen işletmelerin muhasebe kayıtlarının oluşturulması, finansal raporlamanın yapılması ve iş süreçlerinin karmaşıklaşması bilgi sistemlerinin kullanılması ile kolaylaşmaktadır.

İşletmelerin finansal işlemlerde, finansal tabloların hazırlanmasında, tüm iş süreçlerinde bilgi sistemlerinden yararlanması, verilerin işleme, saklanma, aktarılma ve kontrol edilme biçimini değiştirmiştir. Bu nedenle hızlı ve doğru bilgiye ulaşmanın çok önemli olduğu muhasebe ve denetim alanlarında bilgi sistemlerinin kullanımından kaynaklı risklerin dikkate alınması gerekmektedir. Bilgi sistemlerinin yaygın olarak kullanıldığı işletmelerde, finansal tablolar ve diğer finansal bilgiler bilgi sistemlerinin bir çıktısıdır. Bu nedenle finansal tabloların bağımsız denetiminde bilgi sistemlerinin dikkate alınması gerekliliği bilgi sistemleri denetiminin önemini ortaya koymaktadır.

Ülkemizde bilgi sistemleri, Maliye Bakanlığına bağlı, Gelir İdaresi Başkanlığı tarafından e-Fatura, e-Arşiv fatura, e-İrsaliye, e-Defter, e-Bilet, e-serbest meslek makbuzu (SMM), e-Müstahsil Makbuzu gibi uygulamalar ile e-belge başlığı altında kullanılmaktadır. e-Belgelerin elektronik ortamda iletimi, GİB Web Portal, doğrudan entegrasyon veya özel entegrasyon ile sağlanabilmektedir. En çok tercih edilen yöntem özel entegrasyon yöntemidir.

Çalışmanın konusunu Ankara ilinde bulunan bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi konusundaki görüşleri ve e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerinin araştırılması oluşturmaktadır. Bu bağlamda literatür taraması ve GİB tarafından yayınlanmış olup zorunlu tutulan e-Belge Özel Entegratörleri bilgi sistemleri denetimi klavuzu

doğrultusunda hazırlanmış olan anket soruları ile bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşleri ve e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerinin araştırılması amaçlamaktadır. Bu amaç doğrultusunda Ankara ilinde yer alan bağımsız denetçilere yüz yüze anket uygulamalı bir araştırma yapılmış, elde edilen veriler çeşitli istatistiki yöntemlerle analiz edilmiş, ulaşılan sonuçlar paylaşılmıştır.

Anahtar Kelimeler: Denetim, Bilgi Sistemleri Denetimi, Bağımsız Denetim, Özel Entegratör Kuruluşları, Muhasebede Dijitalleşme.



**OPINIONS OF INDEPENDENT AUDITORS ON THE EFFECT OF
INFORMATION SYSTEMS AUDIT ON INDEPENDENT AUDIT,
INVESTIGATION OF THE KNOWLEDGE LEVELS REGARDING E-
DOCUMENT PRIVATE INTEGRATORS INFORMATION SYSTEM AUDIT:
ANKARA PROVINCIAL PRACTICE**

ABSTRACT

In the globalizing world, businesses need to follow and use the opportunities that arise depending on the developments in technology in order to be successful due to the increasing competition. The merging and growth of businesses and the creation of accounting records of growing businesses, the making of financial reporting and the complexity of business processes are facilitated by the use of information systems.

Businesses' use of information systems in financial transactions, and preparation of financial statements, in all business processes, has changed the way data is processed, stored, transferred, and controlled. For this reason, it is necessary to consider the risks arising from the use of information systems in the fields of accounting and auditing, where it is very important to get fast and accurate information. In businesses where information systems are widely used, financial statements and other financial information are an output of information systems. For this reason, the necessity of considering information systems in the independent audit of financial statements reveals the importance of information systems auditing.

In our country, information systems are implemented by the Revenue Administration, affiliated to the Ministry of Finance, with applications (such as e-Invoice, e-Archive invoice, e-Waybill, e-Ledger, e-Ticket, e-self-employment receipt (SMM), e-Producer Receipt) used under the document title (e-). The electronic transmission of e-documents can be achieved through the GİB Web Portal, direct integration, or special integration. The most preferred method is the custom integration method.

The subject of the study is the opinions of the independent auditors in Ankara on the effect of information systems auditing on independent auditing and investigating the knowledge levels of e-document private integrators on information system auditing. In

this context, the obligatory e-document private integrators information systems audit guide published by the GİB and the literature review and survey questions prepared in line with the opinions of independent auditors on the effect of information systems auditing on independent auditing, aiming at the e-document private integrators information system audit. For this purpose, a face-to-face survey was conducted with the independent auditors in Ankara, the data obtained were analyzed with various statistical methods, and the results were shared.

Keywords: Audit, Information Systems Audit, Independent Audit, Private Integrator Organizations, Digitalization in Accounting.



İÇİNDEKİLER

GİRİŞ.....	1
BİRİNCİ BÖLÜM.....	3
1. BAĞIMSIZ DENETİM.....	3
1.1. Bağımsız Denetim.....	3
1.2. Denetim Türleri.....	3
1.2.1. Finansal Tabloların Bağımsız Denetimi.....	4
1.2.2. Uygunluk Denetimi.....	4
1.2.3. Faaliyet Denetimi.....	5
1.3. Bağımsız Denetim Süreci.....	5
1.3.1. Denetim İşinin Alınması.....	5
1.3.2. Müşteri İşletmenin Tanınması.....	6
1.3.3. Önceki Denetçi ile Görüşme.....	7
1.3.4. Denetim Sözleşmesinin İmzalanması.....	7
1.3.5. Denetim Planlaması.....	8
1.3.5.1. İşletme ve İçinde Bulunduğu Sektör Hakkında Bilgi Toplama.....	9
1.3.5.2. İç Kontrol Sistemi Hakkında Bilgi Toplama.....	9
1.3.5.3. Önemlilik Düzeyini Belirleme.....	10
1.3.5.4. Denetim Riski Düzeyini Belirleme.....	11
1.3.5.5. Denetimin Amaçlarını Belirleme.....	12
1.3.5.6. Denetim Programı.....	12
1.3.5.7. Zaman Planlaması.....	13
1.3.5.8. İşgücü Planlaması ve Gözetim.....	13
1.4. Denetim Programının Yürütülmesi, Tamamlanması ve Bulguların Raporlanması.....	14
İKİNCİ BÖLÜM.....	16
2. BİLGİ SİSTEMLERİ VE DENETİMİ.....	16
2.1. Bilgi Sistemleri Temel Kavramlar.....	16
2.1.1. Sistem Kavramı.....	16
2.1.2. Bilgi Sistemleri ve Bilgi Teknolojileri Kavramları.....	16
2.1.3. Bilgi Sisteminin Unsurları.....	18
2.1.3.1. Donanım.....	19
2.1.3.2. Yazılım.....	19
2.1.3.3. Ağ (Network).....	21

2.1.3.3.1. Ağ Topolojileri.....	22
2.1.3.3.2. Ağ Bağlantı Tipleri	23
2.1.3.3.3. Ağ Çeşitleri	23
2.1.3.3.4. Ağ Cihazları	24
2.1.3.3.5. Bilgisayar Ağlarının Katmanlı Yapısı	24
2.1.3.3.6. İnternet – İnternet – Extranet	27
2.1.3.4. Veritabanı.....	27
2.1.3.5. Prosedürler	27
2.1.3.6. İnsanlar.....	28
2.1.4. Bilgi Sistemlerinin Temel Fonksiyonları.....	28
2.1.5. Bilgi Sistemleri Denetçisi	30
2.1.6. Bilgi Sistemleri Denetiminde Riskler	30
2.1.7. Bilgi Sistemleri Denetimi Kapsamında Kabul Görmüş Otoriteler	31
2.1.7.1. Uluslararası Otoriteler ve Düzenlemeleri.....	31
2.1.7.1.1. Uluslararası Sayıştaylar Birliği (INTOSAI)	32
2.1.7.1.2. Uluslararası Muhasebeciler Federasyonu (IFAC).....	32
2.1.7.1.3. Amerikan Sertifikalı Muhasebeciler Enstitüsü (AICPA).....	33
2.1.7.1.4. Uluslararası İç Denetçiler Enstitüsü (IIA)	33
2.1.7.1.5. Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA-Information Systems Audit and Control Association)	34
2.1.8. ISACA Tarafından Yayınlanan Standartlar.....	34
2.1.8.1. COBIT (Bilgi ve İlgili Teknoloji için Kontrol Hedefleri).....	34
2.1.8.2. ISO 27001/27002 Bilgi Güvenliği Yönetim Sistemi	35
2.1.8.3. ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi)	36
2.1.9. Ulusal Otoritelerin Düzenlemeleri ve Standartları	37
2.1.9.1. Sayıştay	37
2.1.9.2. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK).....	38
2.1.9.3. Gelir İdaresi Başkanlığı.....	39
2.1.9.4. Kamu Gözetim Muhasebe ve Denetim Standartları Kurumu	39
2.1.9.5. Sermaye Piyasası Kurulu (SPK)	40
2.2. Bilgi Sistemleri Denetimi ve e-Belge Özel Entegratör Bilgi Sistemleri Denetimi	41
2.2.1. Bilgi Sistemleri Denetimi	41
2.2.1.1. Bilgi Sistemleri Denetiminin Planlanması	43
2.2.1.2. Bilgi Sistemleri Kontrollerinin Değerlendirilmesi.....	44
2.2.1.3. Bilgi Sistemleri Denetim Sonuçlarının Raporlanması ve İzlenmesi.....	48
2.2.2. e-Belge Özel Entegratör Bilgi Sistemleri Denetimi	49
2.2.2.1. Denetim ve Onay Süreci	54
2.2.2.2. Denetimin Planlanması	55
2.2.2.3. Kontrollerin Değerlendirilmesi	56
2.2.2.3.1. Fiziki Güvenlik Şartları ve Tedbirleri.....	57
2.2.2.3.2. Sızma Testleri	60

2.2.2.3.3. Risk Yönetimi	62
2.2.2.3.4. İş Sürekliliği ve Felaket Kurtarma Merkezi (FKM) Yönetimi	63
2.2.2.3.5. Değişiklik Yönetimi	65
2.2.2.3.6. Denetim İzlerinin Oluşturulması ve Saklanması	67
2.2.2.3.7. Dış Hizmet Alımı	67
2.2.2.3.8. Personelin Niteliğine İlişkin Gereksinimler.....	68
2.2.2.3.9. Uluslararası Standartlara İlişkin Sertifikasyonlar	69
2.2.2.3.10. ÖEBSD Değerlendirme Sınıfları.....	69
2.2.2.3.10.1.Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu (ÖEBSD_SER)	69
2.2.2.3.10.2.Personelin Niteliği (ÖEBSD_PER).....	70
2.2.2.3.10.3.Sistem ve Güvenlik Değerlendirme Sınıfı (ÖEBSD_SIS).....	70
2.2.2.3.11. Raporlama	71
2.2.2.3.12. ÖEBSD Raporuna Bağlı Olarak GİB Tarafından Uygulanacak Yaptırımlar	72
2.2.3. E-Belge Özel Entegratörleri Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi	73
ÜÇÜNCÜ BÖLÜM.....	78
3. BAĞIMSIZ DENETÇİLERİN BİLGİ SİSTEMLERİ DENETİMİNİN BAĞIMSIZ DENETİME ETKİSİ KONUSUNDAKİ GÖRÜŞLERİ VE E-BELGE ÖZEL ENTEGRATÖRLERİ BİLGİ SİSTEM DENETİMİNE İLİŞKİN BİLGİ DÜZEYLERİNİN ARAŞTIRILMASI: ANKARA İLİ UYGULAMASI	78
3.1. Araştırmanın Konusu, Amacı ve Önemi	78
3.2. Araştırmanın Evreni ve Örneklemi	79
3.3. Araştırmanın Veri Toplama Yöntemi	80
3.4. Araştırmanın Teorik Modeli ve Hipotezler.....	81
3.5. Araştırmanın Sınırlılıkları	88
3.6. Araştırma Verilerinin Analizi	88
3.7. Araştırma Bulguları ve Yorumlar	89
3.7.1. Sosyo-Demografik Özellikler ile İlgili Bulguların Analizi	89
3.7.2. Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşlerinin Analizi.....	91
3.7.3. Bağımsız Denetçilerin e- Belge Özel Entegratör Bilgi Sistem Denetimi ile İlgili İfadelere İlişkin Bilgi Düzeyinin Analizi	105
3.7.4. Araştırma Hipotezlerinin Analizleri	141
Bağımsız Gruplar T Testi	141
Anova Testi	142

3.7.4.1. Bilgi Sistem Denetimi ile Bağımsız Denetim Arasındaki İlişkiyi Ölçen Hipotezlerin Analizi.....	142
3.7.4.2. Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeylerini Ölçmeye Yönelik Hipotezlerin Analizi..	148
SONUÇ VE ÖNERİLER.....	208
KAYNAKÇA.....	224
EKLER	230



TABLULAR LİSTESİ

Tablo 2.1: Bilgi teknolojileri ve Bilgi Sistemleri Arasındaki Farklar (https://www.geeksforgeeks.org 15.10.2022).....	17
Tablo 2.2: e-Belgelerin elektronik ortamda iletim yöntemleri (Gülten, e-Maliye Muhasebe Uygulamaları Eğitim Notlarından alınmıştır. http://www.esmmmo.org/)	53
Tablo 2.3: Fiziksel ve Çevresel Risk Alanları	57
Tablo 2.4: Fiziksel ve Çevresel Kontroller	58
Tablo 3.1: Aritmetik Ortalamaların Değerlendirme Aralığı	81
Tablo 3.2: Sosyo-Demografik Özellikler ile İlgili Bulguların Analizi	90
Tablo 3.3: Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere İlişkin Görüşlerine Ait Frekans Dağılımları.....	92
Tablo 3.4: Bağımsız Denetçilerin Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili Görüşlerine İlişkin Frekans Dağılımları	106
Tablo 3.5: Bağımsız Denetçilerin İç Kontrol ve Denetim Mekanizmalarına İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	110
Tablo 3.6: Bağımsız Denetçilerin Personelin Niteliğine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	113
Tablo 3.7: Bağımsız Denetçilerin Fiziki Şartlar ve Güvenlik Tedbirlerine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	117
Tablo 3.8: Bağımsız Denetçilerin Erişim Güvenliğine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	121
Tablo 3.9: Bağımsız Denetçilerin İş Sürekliliği, Risk Yönetimi ve Acil Durum Planlarına İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları.....	124
Tablo 3.10: Bağımsız Denetçilerin Denetim İzleri Yönetimine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	128
Tablo 3.11: Bağımsız Denetçilerin Değişiklik Yönetimine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	132
Tablo 3.12: Bağımsız Denetçilerin Dış Hizmet Sağlayıcılarının Yönetimine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	135
Tablo 3.13: Bağımsız Denetçilerin Hizmet Yazılımlarına İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları	138

Tablo 3.14: Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisine İlişkin İfadelere Ait Görüşleri.....	142
Tablo 3.15: Cinsiyete Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisine İlişkin İfadelere Ait Görüşleri İçin T Testi Sonuçları	143
Tablo 3.16: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi İlişkin İfadelere Ait Görüşleri İçin T Testi Sonuçları	144
Tablo 3.17: Yaş Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları	145
Tablo 3.18: Eğitim Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile ilgili ifadeler Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları	145
Tablo 3.19: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	146
Tablo 3.20: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	147
Tablo 3.21: Tukey in HSD Test Sonuçları.....	147
Tablo 3.22: Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri ile İlgili İfadelere Ait Görüşleri	148
Tablo 3.23: Cinsiyete Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin İfadelere Ait Görüşleri İçin T Testi Sonuçları	149
Tablo 3.24: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelere dair görüşlerine ilişkin T Testi Sonuçları.....	150
Tablo 3.25: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları.....	150
Tablo 3.26: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	151

Tablo 3.27: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	152
Tablo 3.28: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları.....	152
Tablo 3.29: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	153
Tablo 3.30: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Denetim İzleri Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	153
Tablo 3.31: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	154
Tablo 3.32: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere Dair Görüşlerine ilişkin T Testi Sonuçları	154
Tablo 3.33: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları.....	155
Tablo 3.34: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin T Testi Sonuçları.....	156
Tablo 3.35: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	156
Tablo 3.36: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile İlgili İfadelere Dair Görüşlerine ilişkin T Testi Sonuçları.	157
Tablo 3.37: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	158

Tablo 3.38: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları.....	158
Tablo 3.39: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	159
Tablo 3.40: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	160
Tablo 3.41: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Denetim İzleri Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları.....	160
Tablo 3.42: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları.....	161
Tablo 3.43: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	162
Tablo 3.44: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları	162
Tablo 3.45: Yaş Durumuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi	163
Tablo 3.46: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile ilgili İfadelerine İlişkin Tek Yönlü Varyans Analizi Sonuçları	164
Tablo 3.47: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile ilgili ifadelerine İlişkin Tek Yönlü Varyans Analizi Sonuçları	164

Tablo 3.48: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	165
Tablo 3.49: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	166
Tablo 3.50: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	166
Tablo 3.51: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları Raporu ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	167
Tablo 3.52: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	168
Tablo 3.53: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	168
Tablo 3.54: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	169
Tablo 3.55: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	170
Tablo 3.56: Eğitim Durumuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi	170
Tablo 3.57: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi Sonuçları	171
Tablo 3.58: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	172

Tablo 3.59: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Personelin Nitelięi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	172
Tablo 3.60: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	173
Tablo 3.61: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Erişim Güvenlięi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	173
Tablo 3.62: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından İş Süreklilięi, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	174
Tablo 3.63: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	175
Tablo 3.64: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Deęişiklik Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	175
Tablo 3.65: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	176
Tablo 3.66: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	176
Tablo 3.67: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi	177
Tablo 3.68: Tukey in HSD Test Sonuçları.....	177
Tablo 3.69: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	178
Tablo 3.70: Tukey in HSD Test Sonuçları.....	179

Tablo 3.71: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından İ Kontrol ve Denetim Mekanizmaları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	180
Tablo 3.72: Tukey in HSD Test Sonuçları.....	180
Tablo 3.73: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Personelin Nitelięi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	181
Tablo 3.74: Tukey in HSD Test Sonuçları.....	181
Tablo 3.75: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	182
Tablo 3.76: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Erişim Güvenlięi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	183
Tablo 3.77: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından İş Süreklilięi, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi	183
Tablo 3.78: Tukey in HSD Test Sonuçları.....	184
Tablo 3.79: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	185
Tablo 3.80: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Deęişiklik Yönetimi Raporu ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi.....	185
Tablo 3.81: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi.....	186
Tablo 3.82: Tukey in HSD Test Sonuçları.....	186
Tablo 3.83: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi.....	187
Tablo 3.84: Tukey in HSD Test Sonuçları.....	188

Tablo 3.85: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi.....	189
Tablo 3.86: Tukey in HSD Test Sonuçları.....	189
Tablo 3.87: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi.....	190
Tablo 3.88: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi.....	191
Tablo 3.89: Tukey in HSD Test Sonuçları.....	191
Tablo 3.90: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Personelin ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	192
Tablo 3.91: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	193
Tablo 3.92: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi	193
Tablo 3.93: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi.....	194
Tablo 3.94: Tukey in HSD Test Sonuçları.....	195
Tablo 3.95: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	195
Tablo 3.96: Tukey in HSD Test Sonuçları.....	196
Tablo 3.97: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları	197

Tablo 3.98: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	197
Tablo 3.99: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları.....	198
Tablo 3.100: Tukey in HSD Test Sonuçları.....	198
Tablo 3.101: Araştırma Hipotezlerinin Sonuçları.....	199



ŞEKİLLER LİSTESİ

Şekil 2.1: Bilgi Sistemlerinin Bileşenleri (Ly-Huong, 2022:1).....	18
Şekil 2.2: Çalışma Sistemi.....	20
Şekil 2.3: OSI modelinin katmanları (www.imperva.com 15.10.2022).....	25
Şekil 2.4: TCP/IP modelinin katmanları (www.imperva.com 15.10.2022).....	26
Şekil 2.5: Bilgi sistemlerin ve bilgi teknolojisi arasındaki ilişki (Angel, 2018:13).....	28
Şekil 2.6: Veri İşleme Süreci (Angel, 2018:14).....	29
Şekil 2.7: Veri İşleme Süreci (KPGM BT Denetim Standartları ve Uygulamaları Araştırma Raporu 2017:22).	36
Şekil 2.8: e-Belgelerin elektronik ortamda iletimi yöntemleri (https://home.kpmg/tr) .	51
Şekil 2.9: Sızma Testi Süreci (lostar.com.tr 21.08.2022).....	60
Şekil 3.1: Araştırmanın Temel Modeli.....	81
Şekil 3.2: Bilgi sistemleri denetimi bağımsız denetimin bir parçasıdır, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekir.	95
Şekil 3.3: Bilgi sistemleri denetimi, bağımsız denetçinin muhasebe ve iç kontrol sistemi ile ilgili yeterli bir anlayış edinmek amacıyla izlediği yöntemleri etkilemez.	96
Şekil 3.4: Bağımsız denetimde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeler. .	96
Şekil 3.5: Bilgi sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkisi vardır.	97
Şekil 3.6: Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.	98
Şekil 3.7: Bilgi sistemlerindeki altyapı yetersizlikleri ve performans sorunlarının bağımsız denetim üzerine etkisi vardır.	98
Şekil 3.8: Bilgi sistemleri kontrol ve denetim faaliyetlerinin yetersizliğinin bağımsız denetime etkisi yoktur.....	99
Şekil 3.9: Bilgi sistemlerindeki veri ve programlara yetkisiz erişimin bağımsız denetim üzerinde etkisi yoktur.....	100
Şekil 3.10: Denetim planı oluşturulurken, denetim riskinin büyüklüğü belirlenirken bilgi sistem denetimi sonuçları dikkate alınmalıdır.	100

Şekil 3.11: Bilgi sistemleri denetiminin de iç kontrol ve denetim mekanizmaları değerlendirmelerinin bağımsız denetim kanıt güvenilirliğine etkisi vardır.....	101
Şekil 3.12: Bilgi sistemleri denetimi şirket verilerine erişimi sınırlayarak yasalara ve muhasebe standartlarına uyumu geliştirir, kontrolleri iyileştirir.	102
Şekil 3.13: Bilgi sistemleri üzerine siber saldırıların bağımsız denetim üzerinde olumsuz etkisi vardır.....	102
Şekil 3.14: Bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki etmez.....	103
Şekil 3.15: Bağımsız denetçi, bilgi sistemlerinin içyapısında bulunan önemli olarak değerlendirilebilecek hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır.	104
Şekil 3.16: Finansal tablolara kaynak verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.....	104
Şekil 3.17: Bilgi Sistemleri Denetimi Üzerine Bağımsız Denetçilere Zorunlu Eğitim Verilmelidir.....	105
Şekil 3.18: Uluslararası standartlara ilişkin güncel sertifikasyonlara sahip olmak bilgi sistemleri kalitesini etkiler.....	107
Şekil 3.19: Sızma testlerinin güncellenmesi, saldırı yöntemlerine göre test edilmesi bilgi güvenliğini etkiler.....	108
Şekil 3.20: Sızma testlerinin kalitesi ya da sayısı bilgi sistemleri kalitesini etkilemez.	108
Şekil 3.21: GİB tarafından saklama hizmeti verme izni almış firmanın, mükellefin e- Belge uygulamaları kapsamında oluşturulan belgelerinin BİS raporuna uygun olarak saklanmasını sağlaması bilgi sistemleri kalitesini artırır.....	109
Şekil 3.22: İç kontrol ve iç denetim dokümanı oluşturulması bilgi sistemleri kalitesini etkilemez.....	111
Şekil 3.23: İç Kontrol Dökümanları ile İş Sürekliliği Belgelerinin Birbiriyle Uyumlu Olması Bilgi Sistemleri Kalitesini Etkiler.....	111
Şekil 3.24: İç kontrol denetimlerinin periyodik biçimde yapılması ve denetim sonuçlarının raporlanması bilgi sistemleri kalitesini etkilemez.....	112

Şekil 3.25: İstihdam edilen personelin öğrenimi ve sertifikasyonlarının göreviyle uygun olması bilgi sistemleri kalitesini etkilemez.....	114
Şekil 3.26: Sistemlerin yönetiminde, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görev ve sorumlulukların ayrılığı prensibinin uygulanması bilgi sistemleri kalitesini artırır.	115
Şekil 3.27: Uygun nitelik ve sayıda personel istihdamı bilgi sistemleri kalitesini artırmaz.	115
Şekil 3.28: Özel Entegratör yönetici ve çalışanlarının kamusal bir görev ifa ettiklerinin bilinci ile hareket etmeleri bilgi sistemleri kalitesini artırır.....	116
Şekil 3.29: Hassas verilerin (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanması bilgi sistemleri kalitesini artırır.	118
Şekil 3.30: Veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin durmasına izin verecek bir yapılanma olmadığının kontrol edilmesi bilgi sistemleri kalitesini artırır.	119
Şekil 3.31: Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gerekliliklerinin sağlanması bilgi sistemleri kalitesini artırmaz.	120
Şekil 3.32: Hassas verilere herhangi bir personelin tek başına erişim yetkisinin olmaması bilgi sistemleri kalitesini artırmaz.	122
Şekil 3.33: Sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtların güvenli biçimde tutuluyor olması bilgi sistemleri kalitesini artırır ...	123
Şekil 3.34: Tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş olması bilgi sistemleri kalitesini artırmaz.	123
Şekil 3.35: Özel entegratörün, bir risk yönetim planı oluşturması bilgi sistemleri kalitesini artırır.....	125
Şekil 3.36: Donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olayların risk yönetim planına dâhil edilmesi bilgi sistemleri kalitesini artırmaz.....	126

Şekil 3.37: Bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet veremez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanması bilgi sistemleri kalitesini artırmaz.	127
Şekil 3.38: Özel entegratörün, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef ve GİB ile haberleşmesinde kullanılan yazılım uygulamalarının veri tabanı motorları ve uygulama kayıt altına alınmış olması bilgi sistemleri kalitesini artırır.....	129
Şekil 3.39: Denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınması bilgi sistemleri kalitesini artırmaz.	130
Şekil 3.40: Denetim İzleri yönetimi için veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl oluştuğunun ve saklandığının kayıt altına alınmış olması bilgi sistemleri kalitesini artırır.	131
Şekil 3.41: Değişiklik yönetimi prosedüründe, bilgi sistemlerinde yer alan tüm donanım ve yazılımın her türlü bakım, yama ve değişikliğinin kapsamda yer alması bilgi sistemleri kalitesini artırır.	133
Şekil 3.42: Özel entegratörün, hizmetlerinde kullandığı, mükellef ve GİB ile entegrasyonu sağlayan yazılımların değişiklik yönetimini yapması bilgi sistemleri kalitesini artırır.....	133
Şekil 3.43: Değişiklik yönetimi için bir prosedür oluşturulması bilgi sistemleri kalitesini artırır.	134
Şekil 3.44: Özel entegratörün, dış hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla denetlemesi bilgi sistemleri kalitesini artırır.	136
Şekil 3.45: Kullanıcıların yaptığı tüm işlemlerin kayıtlarının saklanması bilgi sistemleri kalitesini artırmaz.	136
Şekil 3.46: Özel entegratörün dış hizmet alımını sözleşmeye dayalı yapması bilgi sistemleri kalitesini artırır.	137
Şekil 3.47: Her kullanıcının sadece yetkisi olduğu firma adına fatura gönderebilmesi bilgi sistemleri kalitesini artırır.....	139
Şekil 3.48: Düzenlenen her e-Fatura ve uygulama yanıtında yer alan bilgilerin gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırmaz.....	140

Şekil 3.49: Düzenlenen her e-Arşiv Fatura, e-SMM, e-MM, e-Bilet vb. altyapıda işleyen elektronik belgeler ve oluşturulan her e-Arşiv raporunda yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır. 140

Şekil 3.50: Düzenlenen her e-İrsaliye ve irsaliye yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır. 141



KISALTMALAR

AICPA	:	Amerikan Sertifikalı Kamu Muhasebecileri Enstitüsü
BT	:	Bilgi Teknolojileri
COBIT	:	Control Objectives for Information and Related Technology (Bilgi Teknolojileri ve İlgili Teknoloji için Kontrol Amaçları)
BDDK	:	Bankacılık Düzenleme ve Denetleme Kurulu
BGYS	:	Bilgi Güvenliği Yönetim Sistemi
BİS	:	Bilgi İşlem Sistemleri
BSD	:	Bilgi Sistem Denetimi
BS	:	Bilgi Sistemleri
CIA	:	Certified Internal Auditor (Sertifikalı İç Denetçi)
CISA	:	Certified Information Systems Auditor (Uluslararası Sertifikalı Bilgi Sistemleri Denetçisi)
COSO	:	Committee of Sponsoring Organizations of the Treadway Commission Treadway Komisyonu Sponsor Örgütler Komitesi
GİB	:	Gelir İdaresi Başkanlığı
HSM	:	Hassas anahtar ve verileri koruyan fiziksel, yan kanal ataklarına dirençli, mantıksal ve çevresel güvenlik mekanizmalarına sahip, kendisine dışarıdan yapılacak saldırılara (fiziksel atak, ısı ve gerilim değişimi, vb.) karşı dirençli olan, 3DES, AES, RSA gibi algoritmaları kullanarak kripto işlemlerini gerçekleştirebilen cihaz
IAASB	:	International Auditing and Assurance Standards Board Uluslararası Denetim ve Güvence Standartları Kurulu -

IASB	:	International Accounting Standards Board Uluslararası Muhasebe Standartları Kurulu
IFAC	:	International Federation of Accountants Uluslararası Muhasebeciler Federasyonuna)
IIA	:	Institute of Internal Auditors Uluslararası İç Denetçiler Enstitüsü
INTOSAI	:	The International Organisation of Supreme Audit Institutions Uluslararası Yüksek Denetim Kurumları Organizasyonu
IS	:	Information Systems (Bilgi Sistemleri)
ISACA	:	Information Systems Audit and Control Association Bilgi Sistemleri Denetimi ve Kontrolü Birliği
ISO	:	International Organization for Standardization Uluslararası Standartlar Teşkilâtı
ISO/IEC 20000	:	Bilgi Teknolojileri Servis Yönetimi Standardı
ISO 22301	:	Uluslararası İş Sürekliliği Yönetimi Standardı
ISO/IEC 27001	:	Bilgi Güvenliği Yönetim Sistemi Standardı
ITGI	:	Information Technology Governance Institute Bilişim Teknolojileri Yönetişim Enstitüsü
ITAF	:	Information Technology Assurance Framework Bilgi Teknolojileri Güvence Çerçevesi
ITIL	:	Information Technologies Infrastructure Library Bilgi Teknolojileri Altyapı Kütüphanesi
MS SQL	:	Microsoft Structured Query Language
OSI	:	Open Systems Interconnection (Açık Sistemler Arabağlaşımı)

ÖE	:	Özel entegratör: 509 Sıra No.lu VUK GT uyarınca elektronik ortamda oluşturulmasına imkan verilen belgelerin (e-Belgeler) oluşturulma, imzalanma, iletilme veya saklanmasına ilişkin hizmeti vermek üzere GİB'den yetki almış kuruluş
ÖEBSD	:	Özel entegratör kuruluşları bilgi sistem süreçleri denetimi
SOX	:	Sarbanes-Oxley Yasası
SPK	:	Sermaye Piyasası Kurumu
TCP/IP	:	Transmission Control Protocol/Internet Protocol Gönderim Kontrol Protokolü/ Internet Protokolu
UDS	:	Uluslararası Denetim Standartları
VPN	:	Virtual Private Network Özel Sanal Ağ
WAN	:	Wide Area Network Geniş Alan Ağı
XML	:	Extensible Markup Language Genişletilebilir İşaretleme Dili

GİRİŞ

Her geçen gün hızla gelişen teknoloji tüm alanlarda oldukça etkili olmaktadır ve hayatı kolaylaştırmaktadır. Teknolojideki gelişmelerin getirdiği yenilikler tüm alanlarda değişikliklere neden olmaktadır. Küreselleşmeye bağlı artan rekabet ortamında başarıyı sağlamanın yolu bilgi teknolojilerinde yaşanan değişimleri takip edebilmeye bağlıdır.

İşletmelerinde bu gelişmelere ayak uydurmaları oldukça önemlidir. İşletmelerin rekabet güçlerini artırabilmeleri ve gelişen sermaye piyasalarına girebilmeleri için teknolojideki gelişmelere bağlı olarak ortaya çıkan olanakları takip etmeleri ve kullanmaları gerekir.

Günümüzde işletmelerin finansal gelişim sürecinde büyümesi ve faaliyetlerinin artmasıyla beraber muhasebe kayıtlarına ve finansal tablolarına temel oluşturan işlemler oldukça karmaşıklaşmış, hacim ve sayı olarak çok yüksek boyutlara ulaşmıştır. Bu nedenle muhasebe işlemlerinin kayda alınması ve raporlanması ile işletmelerin iş süreçlerinde teknolojinin kullanılması neredeyse zorunlu hale gelmiştir. İşletmelerin birleşmesi, büyümesi ve büyüyen işletmelerin muhasebe kayıtlarının oluşturulması, finansal raporlamanın yapılması ve iş süreçlerinin karmaşıklaşması elektronikleşen bilgi sistemleri sayesinde kolaylaşmaktadır. Eskiden manuel olarak gerçekleştirilen pek çok işlem artık elektronikleşen bilgi sistemleri ortamında yapılmaktadır. İşletmelerin finansal işlemler, finansal tabloların hazırlanması, tüm iş süreçleri v.b için bilgi sistemlerinden yararlanması nedeniyle bu sistemlere özgü riskleri de dikkate almaları gerekmektedir.

Muhasebe bir bilgi üretme sistemi olarak düşünüldüğünde, muhasebede doğru, zamanlı, anlaşılabilir bilgilerin üretilmesi ortak paydaşlar açısından son derece önemlidir. Bilgi teknolojilerinde yaşanan gelişmelerle birlikte ülkemizde maliyenin elektronik uygulamalarıyla (e- vergi dairesi, e-beyanname, e-defter, e-fatura v.b) artık bu bilgiler eş zamanlı olarak bilgi kullanıcılarına iletilebilmektedir. Muhasebe işlemlerinde yaşanan değişimin denetim üzerinde de etkileri olmuştur. Yapılan değişiklikler muhasebe denetiminde doğru, güvenilir, bilginin zamanında ve düşük maliyetle elde edilmesini kanıtların güvenilirliğinin artmasını, sahte belgelerin azalmasını sağlamıştır. Verilere anlık ulaşım sayesinde faaliyetlerin kontrolünün denetimi kolaylaşmıştır.

Bilgi sistemlerinin muhasebe alanında kullanılması, verilerin saklanması, alınma ve kontrol edilme biçimini değiştirmiştir. Bilgi sistemleri vasıtasıyla otomatik olarak işlenen

verilerin; sisteme hatalı girilmesi, bilgilerin yetkisiz kişiler tarafından ele geçirilmesi, sistemsel hatalardan ötürü verilerin tamamen kaybı gibi pek çok risk ortaya çıkmaktadır. Bu nedenle kullanılan teknolojilere özgü risklerin dikkate alınması gerekliliği ortaya çıkmıştır. Oluşan bu tip hataların tespit edilememesi bilgi kullanıcılarına verilen bilgilerin güvenilirliğini azaltmaktadır. Bu durum bilgi sistemleri denetiminin gerekliliğinin önemini ortaya koymuştur.

Konu ile ilgili literatür incelemesi yapıldığında bilgi sistemleri denetiminin bağımsız denetim üzerine etkisi üzerine yapılan çok az sayıda çalışma mevcuttur. Bu çalışmada tespit edilen bu durum giderilmeye çalışılmıştır.

Araştırmanın amacı aşağıdaki şekilde ifade edilebilir:

- Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşlerini araştırmak,
- Bağımsız denetçilerin e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerini araştırmak,

Bu amaç doğrultusunda yapılan çalışma üç bölümden oluşmaktadır.

Çalışmanın birinci bölümünde bağımsız denetim hakkında genel bilgi, bağımsız denetim türleri ve bağımsız denetim süreci hakkında bilgi verilmiştir.

Çalışmanın ikinci bölümünde bilgi sistemleri temel kavramları, bilgi sistemleri riskleri, bilgi sistemleri denetimi kapsamında kabul görmüş ulusal ve uluslararası otoriteler, bilgi sistemleri denetimi kapsamında yayınlanan standartlar, bilgi sistemi denetimi ve e- belge özel entegratör bilgi sistemleri denetimi hakkında bilgi verilmiştir.

Çalışmanın uygulama kısmını oluşturan üçüncü bölümde “Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi konusundaki görüşleri ve e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerinin araştırılması: Ankara ili uygulaması” adlı çalışmaya ilişkin anket verileri analiz edilmiş ve sonuçlar yorumlanarak önerilerde bulunulmuştur.

BİRİNCİ BÖLÜM

1. BAĞIMSIZ DENETİM

1.1. Bağımsız Denetim

İşletmelerin finansal gelişim sürecinde büyümesi ve faaliyetlerinin artmasıyla beraber işletmede sürdürülen işlemlerin nitelikleri daha karmaşık hale gelmektedir. İşlemlerin karmaşıklaşması ve işletmede yürütülen faaliyetlerin sayılarının hızla artması kayıtlara hatalı olarak geçirilme ihtimalini doğurmaktadır. Oluşan bu tip hataların tespit edilememesi bilgi kullanıcılarına verilen bilgilerin güvenilirliğini azaltmaktadır. Finansal bilgi kullanıcıları, işletme hakkında kararlar alabilmek için güvenilir bilgilere ihtiyaç duymaktadırlar. Ancak bu bilgileri kaynağından elde etme olanağına sahip değillerdir. Bu bilgilerin işletme yönetiminden sağlanması gerekmekte olup, yönetimin tarafsız olmaması bilgilerin güvenilirliği konusunda endişe doğuracaktır. Güvenilir olmayan bilgiler tarafların kararlarını olumsuz olarak etkileyebilecek ve risk doğuracaktır. Bu risklerin asgari seviyeye indirilmesi ve işletme tarafından sunulan bilgilerin güvenilirliğinden emin olunabilmesi için bu bilgilerin tarafsız kişiler tarafından denetlenmesi gereği ortaya çıkmıştır (Selimoğlu vd., 2019:2).

Bilgi kullanıcılarına sağlanan bilgilerin güvenilirliğinin araştırılmasının en etkin yolu, bilgilerin bağımsız bir kişi tarafından denetlenmesi ve doğrulanmasıdır.

KGK'ne göre bağımsız denetim: *“Finansal tablo ve diğer finansal bilgilerin, finansal raporlama standartlarına uygunluğu ve doğruluğu hususunda, makul güvence sağlayacak yeterli ve uygun bağımsız denetim kanıtlarının elde edilmesi amacıyla, denetim standartlarında öngörülen gerekli bağımsız denetim tekniklerinin uygulanarak defter, kayıt ve belgeler üzerinden denetlenmesi ve değerlendirilerek rapora bağlanması”* şeklinde tanımlanmıştır.

1.2. Denetim Türleri

Denetim çalışmalarının temel amacı, belirli bir döneme ait şirket verilerini önceden belirlenmiş kriterler ile karşılaştırmak ve uygunluk derecelerini belirlemektir. Bu nedenle

ulaşılmak istenen amaca göre denetim türü belirlenir ve karşılaştırma kriterleri oluşturulur. Bir denetim çalışmasında ilk olarak karşılaştırmaya konu olan bilgiler belirlenir, sonra denetimin türü seçilir ve son olarak ta karşılaştırma kriterleri oluşturulur. Denetim türleri bu nedenle çok çeşitli ölçütlere göre sınıflandırılmaktadır. Genel açıdan bakıldığında denetim faaliyetleri; finansal tabloların denetimi, uygunluk denetimi ve faaliyet denetimi olmak üzere üçe ayrılır (Uyanık 2001:53).

1.2.1. Finansal Tabloların Bağımsız Denetimi

Denetçilerin uygulamada yoğunlukla başvurdukları denetim türü Finansal Tablolar veya Mali Tablolar Denetimi olarak ifade edilebilmektedir (Çalgan vd., 2008:36). Bu denetimde denetim konusu finansal tablolarda beyan edilen bilgilerdir.

Finansal tabloların bağımsız denetimi ile işletmelerin düzenlemiş oldukları finansal tabloların, denetlenecek işletmenin finansal durumunun faaliyet sonuçlarının, genel kabul görmüş muhasebe ilkelerine göre ayrıca yasalara uygun, doğru olarak belirtilip belirtilmediği konusunda bir görüşe ulaşılır. Finansal tabloları incelerken denetçi, farklı kuruluşların bunları farklı amaçlar için kullanacağını dikkate almalıdır. Çünkü denetim, tüm tarafların gereksinimlerini karşılayan genel amaçlı bir incelemedir (Haftacı, 2018: 7). Bu denetim genellikle dış bilgi kullanıcılarının gereksinimlerini karşılar.

1.2.2. Uygunluk Denetimi

Uygunluk denetimi ile işletmede işletme personeli tarafından yapılan işlemlerin, yetkili bir üst makam tarafından saptanmış kurallara uygun olarak yapılıp yapılmadığı araştırılır. Denetim ölçütleri kanun, tüzük, yönetmelikler ve işletme üst yönetiminin belirlediği politika ve yöntemlerdir. Vergi denetimi bu denetim türüne örnek olarak gösterilebilir (Erdoğan v.d 2018:5)

Uygunluk denetimi sonuçları tüm gruplara değil, ilgili kişi (işletme yönetimi) ve kuruluşlara (vergi idaresi) raporlanır. Bu denetim genel olarak iç denetçiler, gereken durumlarda ise dış denetçiler tarafından yapılır. Denetimde elde edilen sonuçlar, finansal tabloların denetimine rehberlik eder (Haftacı 2018:7). Hem işletme içi bilgi kullanıcılarına hem de işletme dışı bilgi kullanıcılarına yönelik olarak yapılabilir.

1.2.3. Faaliyet Denetimi

Faaliyet denetimi, bir işletmenin organizasyon yapısının, iç kontrol sistemlerinin, iş süreçlerinin ve yönetiminin başarısını belirlemeye yönelik kapsamlı bir faaliyettir. Kaynak kullanımı, verimlilik, etkinlik ve tutarlılık ilkelerine göre değerlendirilir. Uygulama alanı oldukça geniş bir denetim türüdür. İşletmenin örgüt yapısı, üretim yöntemleri, pazarlama politikaları, bilgi işlem faaliyetleri, faaliyet denetiminin inceleme alanları arasındadır. Bu denetim herhangi bir denetçi türü tarafından yapılabilirken, genellikle iç denetçiler ve devlete bağlı kamu denetçileri tarafından yapılır (Bozkurt, 2012: 29).

1.3. Bağımsız Denetim Süreci

Bağımsız denetim süreci, bir denetim kuruluşu tarafından yeterli miktarda ve kalitede kanıt toplamak için tanımlanmış bir denetim organizasyonunun metodolojisidir (Selimoğlu vd., 2019:131).

Denetim süreci birbirini takip eden farklı aşamalardan oluşmaktadır. Bu süreç, denetçinin denetim işini alması ile başlar, denetim işinin planlanması, bu plan dâhilinde denetim çalışmalarının yürütülmesi son olarak denetim görüşünün raporlanıp açıklanmasıyla biter. Aşağıda bağımsız denetim süreci aşamaları hakkında kısaca bilgi verilecektir (Toroslu,2016:69).

1.3.1. Denetim İşinin Alınması

Denetim sürecinin ilk aşaması, müşteri işletmenin denetim talebini değerlendirip kabul etmesi ile başlar. Denetim işletmesi talepte bulunan müşteri işletme yetkilileri ile görüşerek topladığı çeşitli bilgileri değerlendirip işin kabul edilmesine ya da edilmemesine karar verir.

Denetim işletmeleri müşteri kabul politikalarını KGK' dan yetki belgesi alırken hazırlayacakları denetim rehberinde açıklarlar. Denetçinin denetim işini almadan önce dikkate alması gereken unsurlardan biri, müşteri açısından denetimin ilk mi yoksa tekrarlanan bir denetim mi olduğu hususudur. İlk denetimin zorluk derecesi yüksek

olabilirken genellikle tekrarlanan denetimin zorluk derecesi düşük olabilmektedir.

1.3.2. Müşteri İşletmenin Tanınması

Bir denetim sürecinin başlayabilmesi için önce işin alınması gerekir. Denetim firması, topladığı bilgileri inceledikten sonra potansiyel müşteriyi değerlendirir ve görevi kabul edip etmeyeceğine karar verir. Denetim firmaları, kendilerine ulaşan her müşteriyi kabul etmek zorunda değildir. Genel kabul görmüş denetim standartları, bağımsız denetim standartları, müşteri onayından önce gerekli çalışmaların yapılmasını şart koşturmaktadır (Güredin, E., ve Uyar S. 2020:235).

Bir işletmeden denetim talebi geldiğinde, denetim firmalarının işi kabul etmeleri durumunda, yüklenmeleri gerekecek riskleri öngörebilmek ayrıca denetim kapsamı ile planlamasını belirlemek amacıyla gerekli ön araştırma çalışmalarını yapmak zorundadırlar. Yapılacak bu araştırmalarda aşağıdaki işlemler yapılır:

- İşletmenin içinde bulunduğu sektördeki durumu tespit edilir.
- İşletmenin geçmişi genel olarak incelenir.
- Çıkar çevreleri ile ilişkilerin sağlıklı olup olmadığı incelenir. Özellikle kamu kurumları ve düzenleyici otoriteler ile ilişkilerine bakılır.
- Kamu kurumları, düzenleyici otoriteler gibi diğer kurum ve işletmelerle olan ilişkilerin sağlıklı olup olmadığı incelenir.
- Müşteri işletmenin finansal durumu, faaliyet sonuçları ile ilgili bilgi edinmek amacıyla finansal tabloları incelenir.
- Tepe yönetimin dürüstlüğü, ilişkileri, yasadışı faaliyetlerinin olup olmadığı araştırılır.
- Tepe yönetimin denetime bakış açısı ve hangi amaçla denetim istediği araştırılır.
- Müşterinin kabul edilmesi halinde denetçinin toplumdaki itibarına olan etkileri araştırılır.
- Önceki denetçi ile görüşülür.
- Müşteri işletmede denetim esnasında bağımsız bir çalışmanın mümkün olup olmayacağı araştırılır.
- Müşteri işletmenin genel olarak muhasebe sistemi incelenerek denetim

faaliyetlerine etkileri araştırılır.

Denetçi yeni müşterinin kabul edilmesi sürecinde denetim riskini dikkate alarak bu işletme ile ilgili finansal, finansal olmayan her türlü bilgiye ulaşmaya çalışır (Bozkurt, 2012: 87).

1.3.3. Önceki Denetçi ile Görüşme

Yeni bir müşterinin alınması kararı verilirken müşteri işletme hakkında sağlıklı bilgi edinme yollarından biride önceki denetçi ile görüşmektir. Genel Kabul Görmüş Denetim Standartlarına göre, önceki denetçiye başvurabilmek için muhakkak müşterinin onayının alınması gerekir. Ancak onay alındıktan sonra eski denetçi ile görüşülebilir. Onay alınmaması işin reddedilmesi için önemli bir göstergedir. İzin alınabilmesi durumunda önceki denetçiden aşağıdaki bilgiler elde edilmeye çalışılır (Toroslu,2016:70)

- İşten ayrılma nedenleri
- Yöneticilerin dürüstlüğü hakkındaki görüşleri
- Muhasebe ilkelerinin ve muhasebe standartlarının uygulanması açısından yöneticilerin tutumları
- Çalışmaları sırasında karşılaşılan sorunlar
- Denetim çalışmalarının rahat yürütülüp yürütülmediği

İki denetçi arasındaki bilgi paylaşımı gizli olup bu konuda bir açıklama yapılamaz. Denetçi, önceki denetçiden sınırlı bilgi edinmişse işi almadan önce işin kabulü noktasında daha ayrıntılı bir araştırmaya ihtiyaç duyabilir. Eski denetçinin müşteri işletme ile ilgili olarak açıklama yapmaktan kaçınması işin reddedilmesi için geçerli bir nedendir (Toroslu,2016:70).

1.3.4. Denetim Sözleşmesinin İmzalanması

Denetim sözleşmesi, denetçi ile müşteri arasında, denetçiyi müşterinin finansal tablolarının genel kabul görmüş muhasebe ilkelerine uygun olup olmadığını belirlemeye ve bu kararı raporlamaya yükümlü kılan ve karşılığında müşterinin, denetim için gerekli bilgileri ibraz etmek ve ücreti ödemek gibi sorumlu olduğu bir anlaşmadır (Çalgan vd., 2008:49).

Müşteri işletme ile ilgili edinilen bilgilerin irdelenmesi neticesinde, denetçi işin kabul edip edilmemesi hakkında karar verecektir. İş kabul etme kararı alan denetçi, durumu denetim anlaşması mektubu ile müşteri işletmeye iletir. Her iki tarafça imzalanan bu mektup, sözleşme niteliği taşır.

Denetim anlaşmasında yer alan hususlar aşağıdaki gibidir.

- Sözleşmenin amacı ve kapsamı
- Denetimin zamanlaması
- Denetim ücreti ve nasıl ödeneceği
- Yapılacak çalışmaların niteliği ve neler olduğu
- Yapılacak farklı çalışmalar ve ek raporlar istenilirse bunlara ait içerikler
- Denetçinin ve işletme yöneticilerinin imzaları

Mektubun taraflarca imzalanması ve denetçiye iletilmesi ile denetim başlamış olur (Çalgan vd. , 2008:50).

1.3.5. Denetim Planlaması

Denetçi görüşüne ulaşmada temel olacak faaliyetlerin ne şekilde yürütüleceği hakkındaki davranış düzenine denetim planlaması denir. Bu planlama ile amaç; denetim konusunu denetim sahalarına ayırmak, bu sahalara denetçi görevlendirmek, ayrı ayrı denetim sahalarında uygulanacak, denetim yöntem, işlemlerini belirlemek ayrıca denetim faaliyetini zamanlamaktır. Yapılan bu işlemler sayesinde denetçi, denetimini gerçekleştirdiği işletmeyi tanır ve olası riskleri tanımlayabilir (Güredin, E., ve Uyar S. 2020:236).

Denetim sürecinin birinci adımı olan denetim planı ve programının sorumlu ortak baş denetçi tarafından yazılı bir şekilde geliştirilmesi gerekir. Denetçi, risk prosedürlerini, önemli hata riskini, denetim kalitesini belirler. Denetim planı, denetim sırasında meydana gelebilecek değişikliklere her zaman uyum sağlayacak esnek olacak şekilde hazırlanmalıdır. Denetim planı aşağıdaki aşamalardan oluşur (Selimoğlu vd. , 2019:150).

- İşletmenin organizasyonu, üretim süreci, iş akışı vb. hususlarda bilgi edinilmesi
- İşletmeye ait iç kontrol sistemi hakkında bilgi edinilmesi
- Denetim riski ve önemlilik sınırının tespit edilmesi
- Denetim programının oluşturulması

Uygun bir şekilde yapılan denetim planı finansal tabloların bağımsız denetimine pek çok fayda sağlamaktadır. Bu faydalar aşağıdaki gibi sıralanabilir.

- Denetimin etkin ve verimli şekilde yürütülebilmesi için yardımcı olmak
- Olası problemlerin zamanında ortaya çıkarılması ve çözüm üretilmesi hususunda yardımcı olmak
- Denetimin önemli alanlarına dikkatin yoğunlaşması konusunda yardımcı olmak
- Yeterli kanıt elde edilmesine yardımcı olmak
- Denetim maliyetlerini makul düzeyde tutabilmeye yardımcı olmak

Denetim sözleşmesinin düzenlenmesi ile denetim görevi de başlamaktadır.

1.3.5.1. İşletme ve İçinde Bulunduğu Sektör Hakkında Bilgi Toplama

Uluslararası denetim standardı ISA 315, denetçinin mali tablolarda hata ve hile kaynaklı önemli yanlışlık riskini değerlendirmek için iç kontrol sistemi dahil iş faaliyetlerini ve iş ortamını değerlendirmesi gerektiğini öngörmektedir. Bu nedenle etkin bir denetim planı hazırlayabilmek için müşteri işletme ile ilgili bazı bilgilerin elde edilmesi gerekmektedir. Bu bilgiler;

- İşletmenin faaliyet gösterdiği işkolu
- İşletmenin ürettiği ürün ve hizmetler
- İşletmenin hukuki yapısı
- Uygulanan muhasebe politikaları, yöntemleri
- İç kontrol yapısı ile ilgili bilgiler
- Finansal tablo kalemleri ve diğer hususların önemlilik düzeyi

olarak sınıflandırılabilir.

Bağımsız denetçi bu temel bilgileri kendi arşivinden, önceki denetçiden veya bizzat müşteri işletmeden edinir (Erdoğan vd., 2018: 53).

1.3.5.2. İç Kontrol Sistemi Hakkında Bilgi Toplama

Denetimin yürütülmesinin en önemli adımlarından biri, müşteri şirketin iç kontrol yapısını incelemek ve değerlendirmektir. Şirketler, olumsuz olayları proaktif olarak önlemek ve güvenilir bilgi elde etmek için iç kontrol yapısı adı verilen çeşitli politika ve

prosedürler belirler. Yönetim kurulu, yöneticiler ve çalışanlar tarafından yönlendirilen iç kontroller, faaliyetlerin etkinliğini ve verimliliğini, finansal raporlama sistemlerinin güvenilirliğini ve meşruiyetini sağlamak ve bu konuda işletmenin etkin ve verimli bir şekilde çalışması için makul güvence sağlamak üzere tasarlanmış bir yapı olarak tanımlanır. Bu sayede iş hedeflerine etkin bir şekilde ulaşır. İç kontrol sistemi, aşağıda belirtildiği üzere üç unsurdan oluşur.

- Kontrol çevresi (işletmenin örgüt yapısı, yönetim felsefesi, personel politikaları, iç denetim, yönetimin kontrol yöntemleri v.b)
- Muhasebe sistemi (muhasebe işlemlerinin kaydedilmesi, raporlanması v.b)
- Kontrol usul ve yöntemleri (fiziksel kontrol, varlıklara erişim ve onları kullanmada özel yetkilendirme ve fiziksel kontrol)

Denetçi, iç kontrol yapısının unsurlarını incelerken, yönetimin iç kontrollere yönelik tutumlarını inceler ve organizasyon yapısını araştırır. Muhasebe sistemini kontrol eder. İşlemler ve mali tabloları karşılaştırır. İç kontrol sisteminin denetiminin amacı, mali tablolardaki önemli hata, aldatma ve usulsüzlüklerin önlenmesi ve varsa tespit edilmesidir (Tanrıverdi, 2021:25).

1.3.5.3. Önemlilik Düzeyini Belirleme

Önemlilik düzeyi, bağımsız denetimin planlanması, yürütülmesi aşamalarında tespit edilen hataların denetim üzerindeki ve düzeltilmemiş yanlışlıklar varsa bunların finansal tabloların kullanılabilirliği üzerindeki ve denetçinin görüş oluşturulmasındaki etkisinin değerlendirmesinde kullanılır.

Önemlilik, denetimin performansında tespit edilen hataların veya yanlışlıkların ne ölçüde kabul edilebilir olacağını ifade eder. Denetçi, her bir bilanço kaleminin önemliliğini, niteliğini ve miktarını dikkate alarak belirler. Önemlilik, finansal tablo kullanıcılarının kararlarının etkilenmeyeceği hata üst sınırı olarak kabul edilmektedir.

Planlama aşamasında belirlenen önemlilik düzeyi, denetçinin uygulayacağı denetim prosedürlerini, çalışma süresini ve denetçinin elde etmesi gereken denetim kanıt miktarını güçlü bir şekilde etkiler. Örneğin, denetçinin önemliliği düşük olarak belirlemesi, toplamaları gereken denetim kanıt miktarını artıracaktır. Yüksek düzeyde önemlilik kanıt miktarını azaltır. Denetçinin önemliliği düşük tutması, denetçinin tutucu

davranarak birçok yanlışlığı ortaya çıkarmak istediği anlamına gelir. Dolayısıyla, önemlilik ile kanıt miktarı arasında ters bir ilişki vardır (Bozkurt, 2012: 99).

1.3.5.4. Denetim Riski Düzeyini Belirleme

Bağımsız denetçinin uygun bir görüş oluşturamaması denetim riski olarak tanımlanmaktadır. Denetim riski denetçilerin yapmış oldukları bağımsız denetim çalışmaları sırasında önemli hataları tespit edememeleri olasılığıdır. Bu durumun tamamıyla ortadan kaldırılabilmesi mümkün olamayacağından denetçilerden bu riski en aza indirmeleri istenmektedir.

Denetim doğal risk, kontrol riski ve ortaya çıkarma riski olmak üzere üç temel risk bileşeninden oluşur.

Doğal risk (yapısal risk): İşletmenin finansal tablolarının önemli yanlışlık içermesi riskidir. Kurumun iç kontrol yapısıyla ilgili politika ve prosedürlerinin etkisi bu risk değerlendirmesinde dikkate alınmaz. Buradaki amaç finansal tablolara önemli hataların yansımaları eğilimini ortaya koyabilmektir. İşletmenin yapısı, teknolojik gelişmeler, yönetimin dürüstlüğü, personelin değişim hızı gibi unsurlar doğal risk düzeyini etkiler. Bu risk türü denetçinin kontrolünde olmayan ve kendi iradesiyle yok edemeyeceği ya da değiştiremeyeceği risk unsurlarındandır. Bu vb. nedenlerle doğal risk genellikle yüksek olarak değerlendirilir.

Kontrol Riski: Bir işletmenin iç kontrol yapısına ilişkin politika ve prosedürlerin önemli hataları önleyememesi veya ortaya çıkarmaması riskidir. Bu risk, bir işletmenin iç kontrol yapısının etkinliğinin sonucudur. Etkili bir iç kontrol yapısı, kontrolü azaltabilir. Risk ve zayıf iç kontrol yapısı riski artıracığından işletmenin kontrol riskini sıfıra indirmesi imkânsızdır.

Ortaya Çıkarma Riski: Denetçilerin finansal tablolarda önemli hataları tespit edememe olasılığıdır. Bu risk, denetçilerin çalışmalarında uyguladıkları denetim prosedürlerinin etkinliği ile belirlenir. Doğal risk ve kontrol riskinden farklı olarak, bu risk türünde risk belirleme düzeyi denetçinin çalışmasının etkisiyle değişebilir. Bu prosedürü kullanan çok etkili bir denetim bu riski azaltabilir (Güredin, E., ve Uyar, S. 2020: 288).

1.3.5.5. Denetimin Amaçlarını Belirleme

Denetim hedefleri, denetçinin mali tablolar yoluyla yönetim tarafından ileri sürülen iddiaları test edebilmesi için tanımlanmalı ve geliştirilmelidir. Denetim amaçlarının belirlenmesi, denetim planlamasının önemli unsurlarından biri olup müşteri işletmenin finansal tablolarının genel kabul görmüş muhasebe ilkelerine uygunluğunun tespit edilmesidir. Bu amaçla denetçi müşteri işletme iddialarının doğru olup olmadığını ortaya çıkarabilecek çalışmalar yapmaktır. İşletmenin iddialarını araştırmaya yönelik denetim hedefleri; gerçeklik, tamlık, dönemsellik, sahiplik, doğruluk, değerlendirme, sınıflandırma ve açıklama olarak ifade edilebilir (Toroslu,2016:84).

1.3.5.6. Denetim Programı

Denetim programı, denetim çalışmalarının aktif bir şekilde yürütülmesi için denetçinin neyi, ne zaman ve kimlerin yardımı ile yapacağı hakkında verdiği kararların ayrıntılı dökümüdür. Başka bir deyişle denetim programı; denetçinin uygulamak üzere seçmiş olduğu denetim prosedürlerinin türünü, kapsamını, uygulama zamanını ve bunların kimler tarafından yürütüleceğini gösteren yazılı bir listedir (Selimoğlu vd., 2019:167)

Denetim planının bu aşamasında, yapılması planlanan denetim çalışması için ayrıntılı bir denetim programı hazırlanmaktadır.

Denetim programını oluşturmanın avantajları aşağıdaki şekilde sıralanabilir.

- Her denetim yöntemi ile ilgili sorumluluğu belirler.
- Denetim çalışanları arasında dengeli bir iş bölümüne olanak sağlar.
- Denetim düzeni, zaman tasarrufu sağlar.
- Denetim faaliyetini yönetenlerin inceleme ve takip yapmasını kolaylaştırır.
- Gelecek yıllarda yapılacak denetim çalışmaları için kılavuz hizmeti görür.
- Denetim standartlarına, Genel Kabul Görmüş Muhasebe İlkeleri'ne bağlılığı güvence altına alır.

Ayrıntılı bir denetim programının hazırlanması oldukça önemlidir. Denetim programı iyi hazırlanmazsa değişen şartlara uyumu zorlaştırır, bağımsız düşüncüyü engeller ve denetimi otomatik hale getirir.

1.3.5.7. Zaman Planlaması

Denetim programı hazırlandıktan sonra denetim çalışmalarının zaman planlaması yapılır. Denetimin zaman planlaması, ilk ya da tekrarlanan denetim olmasına göre farklılık gösterir. Tekrarlanan denetimin zaman planlamasının daha kolay olduğu ileri sürülür. Her iki durumda da denetim çalışmasında aşağıda belirtilen nedenlerden ötürü bir zaman sıkışıklığı sorunu yaşanabilir.

- Denetçi tarafından birden fazla firmanın denetim işinin üstlenilmiş olması,
- Denetçinin müşterilerden talep ettiği bilgi ve belgelerin çoğunun belirtilen zamanda hazırlanmamış olması,
- Yapılacak çalışmalarda yoğunlaştırma zorunluluğunun yılın ilk aylarında gerçekleştirilmesi,
- Bazı denetim sahalarında öngörülenden daha kapsamlı denetleme zorunluluğunun doğması,
- Denetim esnasında kimi muhasebe uygulamalarının değişikliğe uğraması
- Denetçi yardımcılarının yeterli deneyime sahip olmamaları nedeniyle istenilen şekilde çalışmaları yürütememeleri,
- Denetimi yürüten ekipte değişiklik yapılması

Denetçi seçiminin ve denetim anlaşmasının, mümkün olduğu kadar erken bir tarihte yapılması hem müşteri hem de denetçi açısından faydalıdır. Erken bir tarihte yapılan anlaşma, denetim çalışmalarını kolaylaştırır ve gerçekçi bir zaman planlaması yapılmasına olanak tanır (Çalgan vd., 2008:55).

1.3.5.8. İşgücü Planlaması ve Gözetim

Denetim çalışmalarını yürütecek olan denetim ekibi oluşturulurken, denetim elemanlarının sayısı ve deneyim, teknik bilgi, sorumluluk gibi nitelikleri, denetim süresi ve işin niteliği gibi hususlara dikkat etmek gerekmektedir.

Denetim kuruluşlarında denetim ekibi oluşturulurken aşağıdaki gibi bir seçim yapılır.

- Denetim anlaşmasının tüm sorumluluğunu üzerine alacak sorumlu ortak baş denetçi,

- Denetim programlarının bölümlerinden sorumlu olabilecek ve denetçi yardımcılarının işlerini gözden geçirip onları yönlendiren bir ya da daha fazla kıdemli denetçi,
- Kendilerine verilen görevleri yapan denetçi ve denetçi yardımcıları,

Planlama ve gözetim işlevleri denetim sürecinin her aşamasında vardır ve denetim süresince devam eder. Gözetim, denetim sırasında denetçi yardımcılarının çalışmalarının yönlendirilmesi ve amaca uygun bir denetim çalışmasının tamamlanmasına yardımcı bir işlemdir (Çalgan vd., 2008:55).

1.4. Denetim Programının Yürütülmesi, Tamamlanması ve Bulguların Raporlanması

Denetim programının yürütülmesi aşaması, denetim çalışmalarının detaylı olarak yapıldığı, kanıtların toplanıp değerlendirildiği bir süreçtir. Müşteri işletmenin, iç kontrol sisteminin yapısı ve güvenilirliği hakkında bilgi alınması, finansal tablolardaki hataların önlenmesi, varsa ortaya çıkarılması gerekmektedir.

Denetimin tamamlanmasının ardından denetçi, elde edilen kanıtları ve belgeleri ilişkilendirir, yorumlar ve bir denetim görüşü belirler. Belirlenen bu görüş bağımsız denetim raporu adı altında bilgi kullanıcılarına açıklanır.

Denetim sürecine ilişkin rapor denetçinin görüşünü ortaklara ve diğer bilgi kullanıcılarına iletmesine ve onların müşteri işletmenin mali tablolarına güven duymalarını sağlamasına yardımcı olur. Denetçi sonucu açıklarken sonucu olumlu, olumsuz, şartlı görüş veya görüş bildirmekten kaçınma olarak bildirir. Denetim raporu ile denetçinin ne yaptığı açıklanır ve tespit edilen önemli hususlar hakkında bilgi verilir.

Yukarıda tüm aşamaları açıklanan bağımsız denetimin amacı; finansal raporlama standartlarına uygun olarak, finansal tabloların, işletmenin finansal durumunu, faaliyet sonuçlarını ve nakit akışlarını tüm önemli yönleriyle doğru ve yeterli bir şekilde açıklayıp açıklamadığı konusunda görüş bildirmektir. Bu bağlamda; *“denetçilerin görevi ve sorumluluğu, finansal tabloların önemli hata ve yanlışlıklar içerip içermedikleri hakkında makul güvencede bir yargıya ulaşabilmek için, mesleki şüphecilik yaklaşımıyla, denetimi planlamak, programlamak, kanıt toplamak, kanıtları değerlendirmek ve ulaşılan sonuçları uygun bir şekilde raporlamaktır.”* (Güredin, E., ve Uyar, S. 2020: 292). Bu

süreçte dikkate alınması gereken bir diğer önemli hususta işletmelerde kullanılan bilgi sistemleridir. Çok sayıda işletme, bilgi sistemleri kullanımını her geçen gün daha da artırmaktadır. Bilgi sistemlerinin kullanılması, verilerin saklanma, alınma ve kontrol edilme biçimini değiştirmiştir. İşletmelerin finansal işlemler ve tüm iş süreçlerinde bilgi sistemlerinden faydalanmaları kullanılan teknolojilere özgü riskleri de dikkate almak gerekliliğini doğurmuştur. Bu durum bilgi sistemleri denetiminin gerekliliğinin önemini ortaya koymuştur (Güredin, E., ve Uyar, S. 2020: 292).



İKİNCİ BÖLÜM

2. BİLGİ SİSTEMLERİ VE DENETİMİ

2.1. Bilgi Sistemleri Temel Kavramlar

2.1.1. Sistem Kavramı

Sistem, bir amaca ulaşabilmek amacıyla birbiriyle ilişkili olan iki veya daha çok bileşenin bir araya geldiği yapı olarak tanımlanabilir. Her sistem daha büyük bir sistemi destekleyen alt sistemlerden oluşmaktadır. Her alt sistem bir veya birkaç amacı yerine getirmek amacıyla tasarlanmaktadır. Alt sistemlerde bir değişiklik yapılırken hem sistemin kendisine olacak etkileri hem de diğer alt sistemler üzerindeki olası etkileri dikkate alınmalıdır. Bir alt sistem sadece kendi amaçlarına değil aynı zamanda işletmenin ana amaçlarına da hizmet etmelidir (Romney, M.B., ve Steimbart, P.J. 2020: 29).

2.1.2. Bilgi Sistemleri ve Bilgi Teknolojileri Kavramları

İnsanlar tarafından tasarlanan ve işletme ile ilgili verilerin toplanmasını, depolanmasını, yönetilmesini ve kullanıcılara bilgi olarak sunulmasını sağlayan bilgisayar tabanlı sistemlere “bilgi sistemleri” adı verilmektedir. İşletme yöneticilerinin karar alma sürecinde karşılaştıkları belirsizlik faktörünü azaltabilmenin bilimsel yolu, kendilerine karar ile ilgili geçerli ve güvenilir bilgilerin ulaştırılmasıdır. Bu ise işletmede etkin bir bilgi akış sisteminin oluşturulması ile gerçekleştirilebilir. Bilgi sistemi, operasyonları yönetmek için gerekli ve yararlı olan bilgilerin oluşturulması, girdiden verileri işlemek için sistemin çalışması ve kullanılmasıdır. Bilgi sistemleri bağımsız süreçlerin analizine yardımcı olur ve iş aktivitelerine olanak tanır. Bir organizasyonda karar vermek için doğru bilgi sağlamak önemli bir faktör olarak kabul edilir (<https://www.geeksforgeeks.org> 15.10.2022).

Bilgi teknolojisi, daha hızlı iletişim kurmak, elektronik depolamayı sürdürmek ve iş veya şirket kayıtlarına koruma sağlamak için sistemin çalışması ve kullanılmasıdır. Yazılım, donanım, ağ vb. gibi bilgi işlem teknolojisi ile ilgili her şeyi ifade etmektedir.

Bilgi sistemleri ve bilgi teknolojisi arasındaki fark, bilgi sisteminin bilgi ile ilgili teknolojiyi, insanları ve süreçleri içermesidir. Hem bilgi teknolojisi hem de bilgi sistemleri başkalarıyla çalışmayı içerecek olsa da bilgi sistemleri uzmanları iş hedeflerine ulaşmak için teknoloji ve diğer sistemleri kullanma konusunda genellikle daha fazla entegredir. Bilgi teknolojisi uzmanları, genel organizasyona önemli bir işlev sunarken, daha çok makinelere, donanım ve yazılım sistemlerine odaklanırlar (www.floridatechonline.com 19.09.2022). Bilgi teknolojileri ve bilgi sistemleri arasındaki farklar Tablo 2.1’ de verilmiştir.

Tablo 2.1: Bilgi teknolojileri ve Bilgi Sistemleri Arasındaki Farklar (https://www.geeksforgeeks.org 15.10.2022)

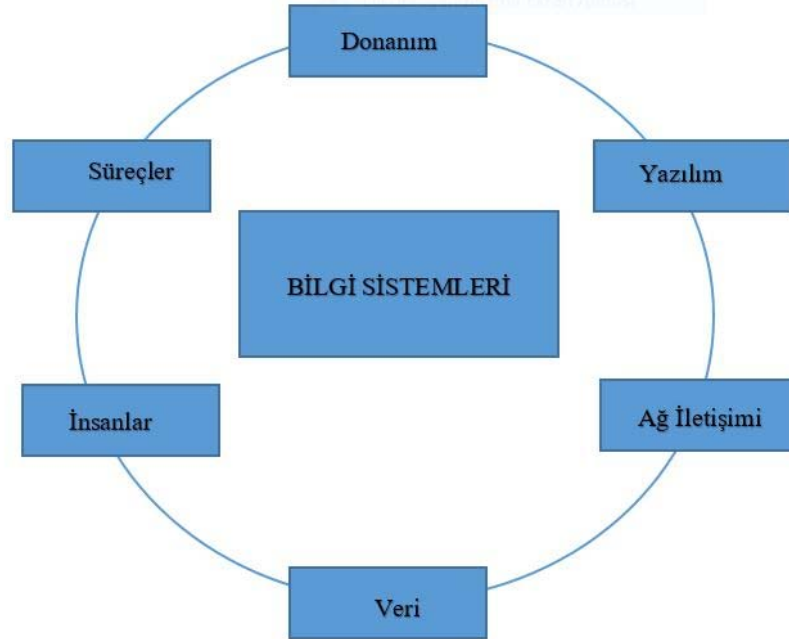
Bilgi Teknolojileri	Bilgi Sistemleri
Bilgi sisteminin bir alt sistemidir	Verileri düzenlemek ve analiz etmek için kullanılan bir yazılımdır.
Temel amacı, insanların işlerini düzgün ve etkili bir şekilde yapmalarına ve bir kuruluş/ işletme içinde hedeflerine ulaşmalarına yardımcı olmaktır.	Temel amacı, ham verileri, organizasyon veya işletme içinde karar vermek için fayda sağlayacak bilgilere dönüştürmektir.
Esas olarak, teknolojiyi kullanarak üretkenliği ve verimliliği artırmaya odaklanırlar.	Esas olarak operasyonlara, yönetime ve karar vermeye destek sağlamaya odaklanırlar.
Genel olarak üç bileşenden oluşur. (Yazılım, Donanım. Ağlar ve veriler).	Genellikle altı bileşenden (donanım, yazılım, ağ iletişimi, veri, insanlar ve süreçler) oluşur.
İnsanların bu sistemden yararlanmasına ve anlamlandırmasına yardımcı olur.	Teknoloji ve insanlar arasında bir köprü görevi görür.
Bilgi sistemi içindeki bilgi veya verileri tasarlar, uygular, sürdürür ve destekler.	Bilgiyle ilgili teknolojiyi, insanları ve süreçleri içerir.
Operasyonel talepleri karşılamak için yeni yazılım güncellemelerinin kullanıma sunulmasını, kullanıcı teknolojisindeki	İnsanların ve süreçlerin, kuruluşlarının performansını nasıl destekleyebileceğini veya engelleyebileceğini ayrıca modern iş

sorunların giderilmesini, eski donanımın değiştirilmesini vb. içerir	ortamlarında bilgisayar ağlarını ve uygulamaları yönetmeyi içerir.
İletişimin uygulanmasına, ticaret ve iş sektörünün kurulmasına ve büyütülmesine, iş itibarının artırılmasına vb. yardımcı olur.	Operasyonel verilerin, iletişim kayıtlarının, belgelerin ve revizyon geçmişlerinin saklanmasına yardımcı olur.

2.1.3. Bilgi Sisteminin Unsurları

Bilgi sistemleri donanım, yazılım, ağ iletişimi, veri, insanlar ve süreçler olmak üzere altı ana bileşene sahip olup Şekil 2.1’de görülmektedir. Bilgi sistemini, bilgi teknolojileri altyapısı oluşturmaktadır.

Şekil 2.1: Bilgi Sistemlerinin Bileşenleri (Ly-Huong, 2022:1)



Her bir bileşenin belirli bir rolü vardır ve tüm rollerin birlikte çalışması ile bilgi sistemleri işlerlik kazanmaktadır. İlk dört bileşen teknoloji olarak gruplandırılabilirken, diğer iki bileşen olan insanlar ve süreçler, kuruluşların hedeflerini yerine getirebilmek için teknolojileri kullanma durumuna göre kuruluşlara değer kazandıran iki bileşendir.

2.1.3.1. Donanım

Bir bilgisayar sistemi donanım ve yazılım olmak üzere iki kategoriye ayrılır. Donanım, bilgi işlem cihazlarının çalışmasını sağlayan fiziksel parçalarıdır. Donanım, sunucular, yönlendiriciler, monitörler, yazıcılar ve depolama aygıtları dahil olmak üzere tüm çevre birimleriyle birlikte bilgisayarların kendisini ifade eder. Donanım; giriş donanımı, işleme ve bellek donanımı, çıktı donanımı ve ikincil depolama donanımı olmak üzere dört kategoriye ayrılır.

Giriş Donanımı: Kullanıcıların bilgisayar sistemine veri girmesi işleminin sağlandığı donanım olup klavye, fare, tarayıcı, dijital kameralar örnek verilebilir.

İşleme ve Bellek Donanımı: İstenilen görevi gerçekleştirmek için veri ve bilgilerin işlendiği ve sunulduğu yerdir. Ayrıca bilgisayarın verileri geçici olarak depoladığı bir çalışma alanıdır. Merkezi işlem birimi (CPU), salt okunur bellek (RAM) işleme ve bellek donanımına ait unsurlardır.

Çıktı Donanımı: İşlenen bilgi ve sonuçları görüntülemeye imkân verir. Ekranlar, yazıcılar (Monitör Ekranı, Yazıcı) örnek olarak verilebilir.

İkincil Depolama Donanımı: Bilgisayar sisteminin verileri ve programları kalıcı olarak depoladığı yerdir. Sabit disk, CD sürücü, DVD sürücü gibi parçalar ikincil depolama donanımı olarak sıralanabilir.

Donanım cihazları herhangi bir hasar gördüğünde yenisiyle değiştirilebilir. Kullanıcıların yazılımla ara yüz oluşturmalarına yardımcı olur ve ayrıca gerçekleştirilen görevlerin sonucunu görüntüler.

2.1.3.2. Yazılım

Bilgi sisteminin ikinci bileşeni yazılımdır. Bilgisayar donanımında kullanılan çeşitli programlara yazılım denir. Yazılım donanımın belirli bir dizi görevi verilen talimata uygun olarak yerine getirmesini sağlar. Yani verileri toplar, düzenler, işler ve yönergeleri yerine getirir. Aslında yazılım donanıma bir dizi talimat veren, bir programlama dili kullanarak geliştirilmiş komutlar zinciridir. Bilgisayar programcıları, donanıma ne yapılacağını belirten bir talimat listesi girmek için belirli bir süreci izleyerek yazılım programları oluştururlar. Windows 10, Adobe Photoshop, Google Chrome gibi

örnekler yazılım programlarıdır. Yazılımın düzgün çalışması için donanımda kurulu olması ve benzer şekilde yapılacak işler için donanımın mevcut olması gerekir. Yazılım, programlama süreci ile oluşturulur. Donanım fiziksel bir yapı olup yazılım ise donanıma talimatlar bildiren programdır. Yazılım olmadan, donanım işlevsel olamaz. Her ikisi de birbirine bağımlı olmakla birlikte aynı zamanda birbirlerinden farklıdırlar. Yazılımlar işletim sistem yazılımı ve uygulama yazılımları olmak üzere iki kategoride sınıflandırılabilir. İşletim sistemleri donanımı yönetir ve donanım ile kullanıcı arasındaki arabirimi oluşturur. Uygulama yazılımları, kullanıcı için faydalı birçok şey yapan programlardır. Şekil 2.2' de bu kategoriler görülmektedir (Ly-Huong, 2022:2)

Şekil 2.2: Çalışma Sistemi



İşletim sistemi yazılımı, programcıların temel donanımın özelliklerini öğrenmesini önlemek için donanım ve uygulama arasında bir arabirim sağlar. Örneğin; masa üstü cihazlar için işletim sistemleri Apple macOS, Microsoft Windows ve uygulamalar Adobe Photoshop, Microsoft Excel, Google Haritası iken mobil cihazlar için işletim sistemleri

Google Android, Apple iOS ve uygulamalar mesajlaşma, google haritası vb. olarak verilebilir.

İşletim Sistemi: İşletim sistemi yazılım ve donanım arasında iletişimi sağlayan ve bir önyükleme programı tarafından bilgisayara yüklendikten sonra, bilgisayardaki diğer tüm uygulama programlarını yöneten programdır. Uygulama programları, tanımlanmış bir uygulama programı arabirimi aracılığıyla hizmet isteklerinde bulunarak işletim sisteminden yararlanır. Ayrıca kullanıcılar, komut satırı arabirimi veya grafik kullanıcı arabirimi gibi bir kullanıcı arabirimi aracılığıyla işletim sistemiyle doğrudan etkileşim kurabilir. İşletim sistemleri, bilgisayar yazılımı ve yazılım geliştirmeye güçlü faydalar sağlar.

İşletim sistemleri bilgisayar programlarını çalıştırır ve bilgisayarın başlatma sürecini düzenler. Windows İşletim Sistemi, MacOS (Apple OS X) İşletim Sistemi, UNIX İşletim Sistemi, Linux İşletim Sistemi, Pardus İşletim Sistemi, Android İşletim Sistemi, İOS İşletim Sistemi gibi işletim sistemleri en önemli işletim sistemleridir.

Uygulama Yazılımları: Bu yazılımlar belirli bir görevi veya bir dizi görevi gerçekleştirmek için tasarlanmıştır. Kullanıcı tarafından tasarlanmış (kullanıcının ihtiyaçlarına özel) ya da hazır uygulama yazılımı olabilirler. Uygulama yazılımlarına PowerPoint, Instagram, Whatsapp, Facebook, Paint, Tally vb. yazılımlar örnek olarak verilebilir (<https://www.toppr.com> 10.06.2022).

2.1.3.3. Ağ (Network)

Çeşitli kaynaklar arasında bilgi aktarımının sağlanabilmesi, kaynakların insanlar tarafından paylaşılabilmesi ve insanların zaman ve yer kısıtlaması olmadan birbirleri ile iletişim kurabilmesi bilgisayar ağları kavramını daha da önemli hale getirmektedir. Bir bilgisayar ağı, birbirine bağlı bilgisayarlar, yazıcılar ve diğer cihazlardan oluşur.

Bilgisayarların birbirleriyle haberleşebilmeleri ve veri aktarabilmeleri için aralarında bir bağlantı, genellikle bir kablo aracılığıyla kurulan her şeye ağ (network) denir. Elektrik veya optik iletim sistemleri ile bilgisayarlar arası iletişim sağlanır. Bir ağda verinin iletilmesi için Server (Sunucu Bilgisayar), Client (İstemci) ve Circuit (devre) olmak üzere üç temel donanım bileşeni gereklidir.

Server (Sunucu): İstemci bilgisayar tarafından ağ üzerinde ulaşılan ve program veya istenilen bilgiyi diğer istemci bilgisayarlara paylaşan/dağıtan donanıma veya yazılımlara verilen genel addır. Yani sunucu, ağa bağlı bilgisayarlara bilgiyi ve gerekli hizmeti vermek için bir yazılım uygulamasını çalıştıran bilgisayarı ifade etmektedir. Sunucular herhangi bir bilgisayar ağına bağlı olarak tüm ağ birimlerine yönetim merkezliği yapar ve bilgi dağıtımını gerçekleştirir. Bir ağda sunucunun temel fonksiyonu istemcinin isteklerini servis vermektir. Sunucu merkez durumunda olup bilgiye erişim için yetkileri belirler. Genelde sunucular yüksek performanslı sistemlerdir.

Client (İstemci Bilgisayar): Bir bilgisayar ağında sunucunun bilgi veya hizmetini talep eden sunucudan hizmet alan kullanıcı bilgisayarlarıdır. İstemci sistemler, sunucuya bir istek gönderir ve sunucu istemciye istenilen bilgileri iletir.

Circuit (Devre): Sunucu veya istemci bilgisayar arasında bağlantıyı sağlayıp iletişimin oluşmasını sağlayan elektrik veya optik iletim sistemleridir (Çölkesen, R., ve B. Örencik, 2012:113).

2.1.3.3.1. Ağ Topolojileri

Topoloji çok sayıda bilgisayarın birbirlerine nasıl bağlandıklarını açıklayan genel bir terimdir. Gönderici ve alıcı aracılığıyla düğümleri ve bağlantı hatlarını içeren bir ağın düzenlenmesine ağ topolojisi denir. Bilgisayar ağlarında ağın çizimini belirtir. Fiziksel topoloji ve mantıksal topoloji olmak üzere ağ topolojileri ikiye ayrılmaktadır. Fiziksel topoloji ağda bulunan cihazların ve bunları birbirine bağlayan bütün bağlantıların çizimine verilen isimdir. Mantıksal topoloji ise ağda çerçevelerin bilgisayarlar arasında dağıtım sırasında takip edilen yolun görünümünün çizimi olarak tanımlanır. Fiziksel Ağ topolojileri; Noktadan noktaya topoloji, Yol (Bus) topolojisi, Yıldız (Star) topolojisi, Ağaç (Tree) topolojisi, Halka (Ring) topolojisi olarak sınıflandırılabilir. Mantıksal topolojisi ise noktadan noktaya mantıksal topoloji, çoklu erişim mantıksal topoloji, halka mantıksal topoloji olmak üzere üç şekilde sınıflandırılır (Kara, 2019:130-132).

Noktadan Noktaya topolojisi: En basit topoloji olup iki düğüm noktasını ortak bir bağlantıyla doğrudan birbirlerine bağlar.

Yol (Bus) Topolojisi: Tüm terminaller birbirlerine sadece bir doğrusal kablo ile bağlanmaktadır. Bu sistemde iletilen sinyaller tüm terminallere ulaşır. Sinyal, hedefe

ulařana veya sonlandırıcıya ulařana kadar hat boyunca ilerler. Veri akıřı çift yönlü olup bilgi, hat üzerinde her iki yönde de hareket eder. Ancak bu topolojide birden fazla istasyon veri iletiyorsa ađ trafiđi kesintiye uđrar.

Yıldız (Star) Topolojisi: Yıldız topolojisi yaygın kullanılan bir topoloji tipi olup bilgisayar ađ iletişiminin gerçekteşebilmesi için switch, hub gibi merkezi birim adı verilen cihazlara bađlanmaktadır. Gönderilmekte olan sinyal önce merkez birime daha sonra istenilen hedefe iletilir.

Ađaç (Tree) Topolojisi: Genellikle yıldız topolojisinde bulunan ađları birbirine bađlamada kullanılır.

Halka (Ring) Topolojisi: Sinyalin hedefe ulařıncaya kadar tüm birimlere uđradıđı bir daire řeklindeki bütün düđümlerin birbirine bađlandıđı topoloji türüdür (Kara, 2019:130-132).

2.1.3.3.2. Ađ Bađlantı Tipleri

Ađ bađlantı tiplerinin ařađıda belirtildiđi gibi iki tür ađ bađlantısı vardır.

Kablolu Ađ: Ađda bulunan cihazların birbirleri ile kablo vasıtasıyla bađlandıkları yapıdır. Kablo uzunluđunun fazla olması iletişim performansını kötü yönde etkilemektedir. Kablo türü oldukça önemlidir.

Kablosuz Ađ: Ađdaki cihazların birbirleri ile radyo frekans teknolojisi kullanarak bilgi alışveriři yaptıđı bir ađ yapısıdır.

2.1.3.3.3. Ađ Çeřitleri

Ađ çeřitleri kullanım alanlarına göre yerel alan ađları, geniş alan ađları, özel sanal ađlar olarak sınıflandırılmaktadır.

Yerel Alan Ađları (LAN- Local Area Network); Sistemlerin aynı ortamda ya da yakın mesafelerde olması ana unsurdur. Belli bir alan içerisinde belirli sayıdaki bilgisayarların oluşturduđu bir ađ türüdür. Sistemler arasında kablo ile bađlantı yapılabilir veya düşük güçlü kablosuz bađlantı kullanılabilir.

Geniş Alan Ađları (WAN- Wide Area Network); Ađda bulunan kullanıcı sayısının artması ve ađın alanının genişlemesi sonucu meydana gelen bir ađ türüdür.

Yerel alan ađları ile kampüs türü ađları birbirine bağlamada kullanılmaktadır. Geniş kapsamlı bir ađ sistemi olup birbirinden oldukça uzak olan bilgisayarların bağlanmasıyla oluşturulan bir ađ tipidir (Çölkesen, R., ve B. Örencik, 2012:128).

Özel Sanal Ađlar (VPN); Kullanıcıların internet gibi halka açık ađlar aracılığıyla şirketlerinin kaynaklarına güvenli bir ortamda erişmelerini sağlayan bir ađ türüdür.

2.1.3.3.4. Ađ Cihazları

Bir ađın oluşturulması için uç sistem konumunda olan bilgisayarların birbiri ile iletişim kurmalarını ve karşılıklı çalışmalarını sağlayan ađ cihazlarıdır. Bilgisayarların ve diğer cihazların bir ađa bağlanmasını sağlayan ađ arabirim (NIC- Network Interface Card) kartları, ađ içindeki aygıtların ortak kullanım veya paylaşım için birbirine bağlanmasını sağlayan ve diğer bilgisayarlardan gelen verileri filtreleyerek sadece ilgili bilgisayara gönderen anahtar/dađıtıcı (Switch) cihazlar, ađlar üzerinde yönlendirmeyi yapan yönlendirici (Router) cihazlar, bilgisayarın telefon hatlarını kullanarak iletişim kurmasını sağlayan modemler, kablolu bir internet ađına kablosuz erişimi sağlayan erişim noktası (Access Point) cihazlar ađ cihazları olarak adlandırılır (Çölkesen, R., ve B. Örencik, 2012:129).

2.1.3.3.5. Bilgisayar Ađlarının Katmanlı Yapısı

Ađ sisteminde bilginin bir noktadan diğer bir noktaya nasıl iletildiđi oldukça önemlidir. Veriler ađ üzerinden iletirken oldukça karmaşık işlemler olmaktadır. Bilgisayar ađları konusunda üretim yapan firmalar arasında ortak bir birlik oluşturmak, ađ işleyiş biçimini basitçe tanımlayabilmek protokoller arası etkileşimi belirlemek ve bu alanda çalışan kişiler arasında ortak bir ađ oluşturarak bu işlemlerde kolaylık olsun diye katmanlı yapı kullanılmaktadır (Kara, 2019:13).

2.1.3.3.5.1. OSI Modeli

Uluslararası standart kuruluşu (OSI) tarafından oluşturulmuş model olan OSI modeli, 7 katmanlı bir yapıdan oluşmakta olup her bir katman farklı görevlere sahiptir.

Bu katmanlar iletişimin yapılma biçimini ve diğer katmanlar ile etkileşimin nasıl olacağını açıklar. Bu katmanlar; yazılımların program taleplerini karşılayan uygulama katmanı (application layer), veri biçimlerinin dönüştürüldüğü sunum katmanı (Presentation Layer), iletişim kuran bilgisayarlar arasında ulaştırma sağlayan oturum açan ve sonlandıran oturum katmanı (Session Layer), bilginin nasıl gönderileceğinin belirlendiği aktarım katmanı (Transport Layer), farklı ağ segmentinde olan sistemlerin birbirlerini nasıl bulacağını açıklayan, veri paketinin ağ içindeki hareketini sağlayan ağ katmanı (Network Layer), Yerel sistemler arasında topoloji ile haberleşme özelliğini tanımlayan, donanım adreslerini dönüştüren ve veri akışını düzenleyen veri bağı katmanı (Data Link Layer), verinin sayısal rakamlara dönüştürülmesiyle aktarıldığı fiziksel katman (Physical layer) olmak üzere yedi çeşittir. OSI modelinin yedi katmanı sırasıyla Şekil 2.3’de yer almaktadır.

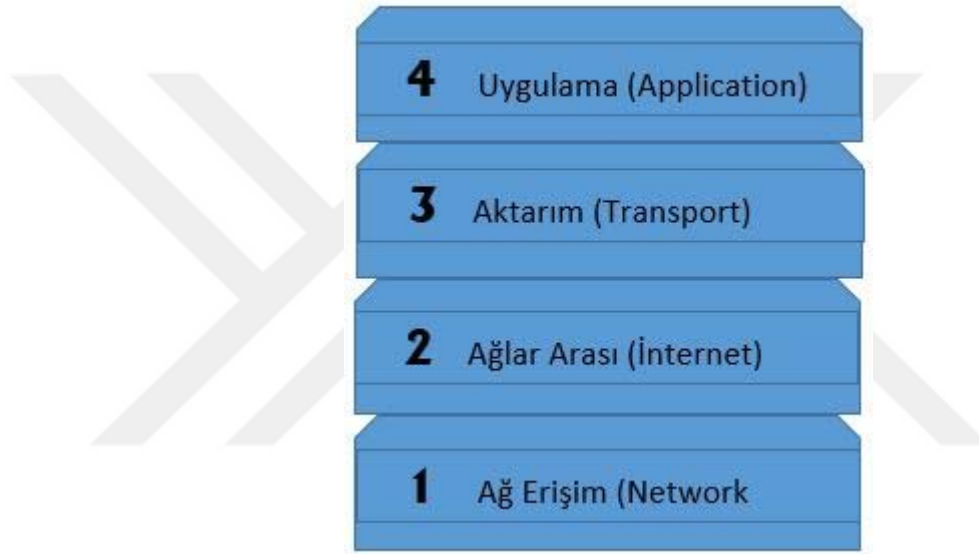
Şekil 2.3: OSI modelinin katmanları (www.imperva.com 15.10.2022)



2.1.3.3.5.2. TCP/IP Modeli

TCP/IP (Transmission Control Protocol/Internet Protocol), veri iletişim protokolünün genel adı olup en yaygın protokol kümesidir. İnternet, TCP/IP katmanlı ağ yapısında bulunmakta olup OSI standartlarına uygun düzenlenmiş olan uygulama, aktarım, ağlar arası ve fiziksel olmak üzere dört çeşit katmandan oluşmaktadır. Şekil 2.4’de TCP/IP modelinin katmanları sırasıyla verilmiştir.

Şekil 2.4: TCP/IP modelinin katmanları (www.imperva.com 15.10.2022)



Uygulama katmanı (Application Layer): Kullanıcı verilerinin hazırlanması, verilerin sıkıştırılması ve şifrelenmesinden sorumlu olan bu katman kaynak ile hedef arasında oturumun kurulmasını ve yönetilmesini sağlar.

Aktarım katmanı (Transport Layer): Uygulama katmanı ile ağ katmanı arasında geçişi düzenleyen, bilgi güvenliği iletimi, bilgi iletimi sırasında hizmet servis ayarları, iletim sonrası bilgilerin hata kontrolü gibi işlemlerin tamamının yapıldığı katmandır.

Ağlar arası katman (Internet Layer): Farklı ağlar arasında iletişimin yönlendirilmesini sağlamaktadır. IP (internet protocol), ARP (adresresolution protocol), ICMP (internet control message protocol) protokollerinden oluşan veri paket yönlendirilmesi ve istenilen yere iletilmesinden sorumlu katmandır.

Ağ Erişim katmanı (Network): Fiziksel adresleme oluşturarak ağdaki hedefe veri gönderiminden ve fiziksel bağlantıların oluşturulmasından sorumludur. Veri bağı ve

fiziksel katmanlardan oluşan fiziksel donanımın bulunduğu katman olup internet katman bağlantısını yapar (Çölkesen, R., ve B. Örencik, 2012:347).

2.1.3.3.6. Internet – Intranet –Extranet

İntranet (iç ağ), şirket çalışanları arasında bilgi paylaşımını sağlayan ve iş süreçlerini düzenleyen ve iş birliğini kolaylaştıran dâhili ağdır. Erişim izni olmayan kullanıcılar kullanamazlar. Bir tarayıcı ortamından erişilebilen intranet, dünyanın her yerinden istenildiği zaman erişilebilecek tüm önemli bilgiler için güvenli bir merkezi depo görevi görür. Extranet (dış ağ) müşteriler, iş ortakları veya şirket dışındaki kişilerin ağa erişmeleri için kullanılır. Extranet tasarımı, şirket dışındaki kişilerle iletişim halinde kalınmasını sağlar. Ancak harici kullanıcılara genellikle iç ağa sınırlı erişim verilir. İnternet, bilgi paylaşmak için birbirine bağlı binlerce bilgisayardan (sunucu ve istemci) oluşan bir genel ağ'dır. Bilgisayar ağlarının kümeleri, dünya çapında bir ağ oluşturmak için birbirine bağlanır. İnternet, dünyanın en büyük iletişim ve bilgi alışverişi aracıdır (Curtis G., ve Cobham D. 2005:205).

2.1.3.4. Veritabanı

Birbiri ile ilgili verilerin kullanım amacına uygun olarak düzenlenerek depo edilmelerine veri tabanı denilmektedir. Ayrıca veri tabanı uygulama programları vasıtasıyla verilerin depolandığı, ulaşılabilirdiği, güncellenebildiği ve silinebildiği bir fiziksel ortamdaki veri topluluğu olarak ta tanımlanabilir (Çelik, A.İ., 2016:2). Bir başka deyişle veritabanı, bilgisayar sisteminde elektronik olarak depolanan yapılandırılmış bir bilgi veya veri topluluğu olarak ta tanımlanabilir (<https://www.oracle.com> 25.09.2022). Veritabanı elektronik depolamayı ve verilerin işlenmesini destekler ve veri yönetimini kolaylaştırır.

2.1.3.5. Prosedürler

Prosedürler, işlerin nasıl yapıldığına ilişkin kuralları, açıklamaları ve talimatları içermektedir. Bilgisayar tabanlı bilgi sistemlerinde prosedürler, donanım, yazılım ve verilerin kullanılma şeklini belirlemektedirler (www.techwalla.com 18.10.2022).

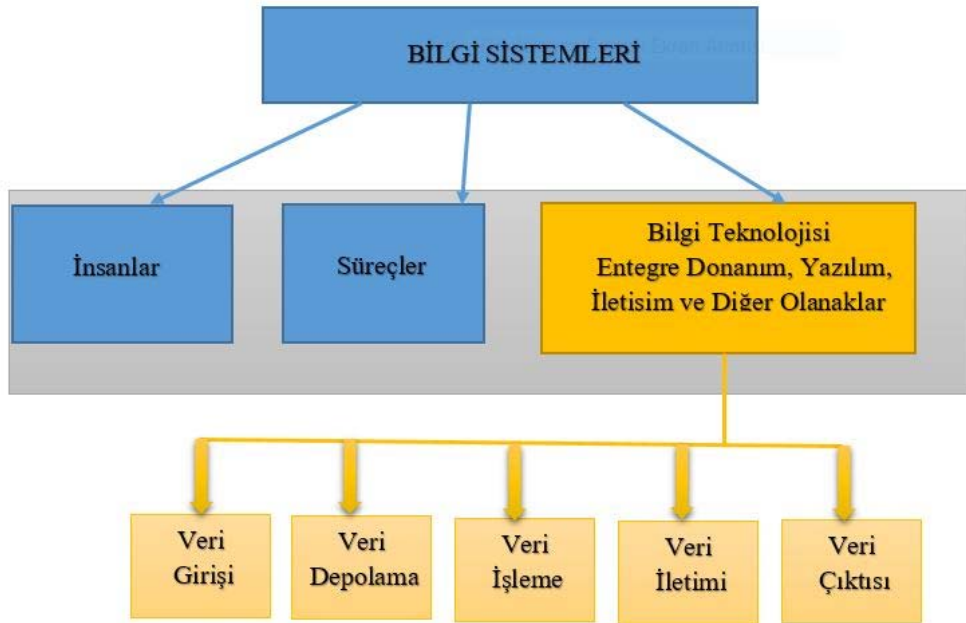
2.1.3.6. İnsanlar

İnsanlar bilgi sistemlerini geliştirmekten ve işletmekten sorumludurlar. Bilgi sisteminin son kullanıcısı insanlar olup kendi amaçları için üretilen bilgileri kullanırlar. Bilgi sisteminin temel amacı son kullanıcıya fayda sağlamaktır.

2.1.4. Bilgi Sistemlerinin Temel Fonksiyonları

Bilgi sistemleri girdi, depolama, işleme, iletme ve çıktı olmak üzere beş farklı fonksiyondan oluşur. Girdi iki kısımda yapılır, bilginin girişi depolanır, işlenir ve daha sonra sistemin çıktısının temelini oluşturur. Kullanıcının sistemden ne tür bir analiz istediğini de sisteme söylemesi gerekir. Bu kısım bilgi teknolojisi departmanı tarafından yapılır ve kullanıcılar tarafından kullanılamaz. Bilgi sistemleri ve bilgi teknolojisi arasındaki ilişki Şekil 2.5’de verilmiştir.

Şekil 2.5: Bilgi sistemlerin ve bilgi teknolojisi arasındaki ilişki (Angel, 2018:13)



Bilgi giriş cihazları (klavye, fare, tarayıcı vb.) aracılığıyla bilgisayar ortamına aktarılır. Bu işleme veri giriş süreci denir. Bilgi sistemlerine bilgilerin doğru ve geçerli bir şekilde girilmesiyle güvenilir bilgi elde edilir. Günümüzde bilgi sistemlerine veri girişi

çeşitli teknikler kullanılarak yapılabilmektedir. Örnek olarak; barkod sistemleri, RFID (Radio Frequency Identification Technology -Radyo Frekanslı Tanımlama Teknolojisi), elektronik veri alışverişi, terminal cihazları, görüntü tarama ve işleme cihazları, ses tanıma sistemleri verilebilir. Farklı ortamlarda ve farklı kaynaklardan veri girişi gerçekleştiğinde, veri girişi sürecinde farklı kontrol mekanizmaları devreye girer.

Bilgisayar ortamında veri girişi yapıldıktan sonra istenilen formatta çıktı birimlerine aktaran bir veri işleme süreci gerçekleşir. Veri işleme süreci, kaydetme, sınıflandırma, hesaplama, özetleme, kaydetme, canlandırma, sunma, iletme işlevleriyle gerçekleşir. (Çelik A., ve Akgemci T. 2010: 25) Veri işleme süreci Şekil 2.6 'da gösterilmiştir.

Bilgi sistem ortamına aktarılan ve veri işleme işlemleri gerçekleştirildikten sonra oluşturulan bilgilere çıktı denir. Bu bilgi sistem adımındaki son adımdır. Çıktı örnekleri, güncellenmiş veri dosyaları, bilgisayar ekranındaki görüntüler, belirli raporlar ve belgelerdir.

Şekil 2.6: Veri İşleme Süreci (Angel, 2018:14)



2.1.5. Bilgi Sistemleri Denetçisi

Bilgi sistemleri denetimi bilgi sisteminin işleyişini ve kuruluşun genel işlerini sürdürmek amacıyla potansiyel risklerin tanımlanması ve analizi, bunların azaltılması veya ortadan kaldırılmasıyla ilgilidir. Denetim gerekli teknik bilgi, uzmanlığa sahip kişiler tarafından gerçekleştirilir. Daha önceleri bu denetimi yapan kişiler bilgi teknolojileri denetçisi ya da bilgi işlem denetçisi olarak adlandırılmış olup günümüzde bu denetimi yapan kişiler bilgi sistemleri denetçisi olarak isimlendirilmektedir (<https://www2.deloitte.com>).

Bilgi sistemleri denetçileri, Bilgi Sistemleri Denetim ve Kontrol Derneği (ISACA) kuruluşunun üyeleri olup Uluslararası İç Denetçiler Enstitüsü (IIA) tarafından düzenlenen standart, ilkeler hakkında yeterince bilgiye sahip kişilerdir. Denetçi, denetimin amacını, kapsamını ve niteliğini anlamalıdır. Denetçi, denetimin neden yapıldığını, denetçinin hangi niteliklere sahip olması gerektiğini, denetimi yapmak için hangi standartların bulunduğunu, en iyi uygulamalarda hangi yöntem ve yaklaşımların yer aldığını bilmelidir. Bir bilgi sistemi denetçisi, denetimini bilgi sistemleri standartlarına göre gerçekleştirebildiği ölçüde, objektif ve oldukça kabul edilebilir sonuçlar ve öneriler içeren raporlar sunabilir. ISACA tarafından düzenlenen CISA sertifikasına sahip bilgi sistemleri denetçileri, denetim sırasında diğer denetimlere benzer denetim prosedürlerini uygular, yeterli ve geçerli kanıt toplar, denetlenen ortamın yeterliliğini ilgili bilgi sistemleri denetim standartları çerçevesinde inceler ve ekleyerek görüş bildirir ve inceleme sürecinin sonunda rapor eder. Bilgi sistemleri denetçisi, teftiş dosyasında bulunan eksikliklerin sebepleri, sistem üzerindeki etkileri, ileride oluşabilecek olumsuz etkiler ve faktörlerin düzeltilmesi hakkında önerilerde bulunur (Böcek, 2014: 23).

2.1.6. Bilgi Sistemleri Denetiminde Riskler

ISACA tanımına göre, bilgi sistemleri denetim sürecindeki denetim riski, "*denetim bulgularına dayanarak yanlış sonuca/görüğe ulaşma riski*" dir. Bir denetim sırasında toplanan kanıtların yanlış veya eksik olma riski her zaman vardır. Denetim sonrası sunulan rapor bu verilere göre hazırlandığından rapor yanlış sonuçlar verir. Bu bir denetim riskidir. Denetim riski aşağıda sunulan üç bileşenden oluşmaktadır.

Doğal Risk: Bilgi sistemleri denetimi için doğal risk tanımı "*ilgili bir iç kontrol sisteminin olmadığı farz edilirse, denetim alanında hata yapılabilme duyarlılığı*" olarak ifade edilmektedir. Uygun kontrollerin tanımlanmadığı bilgi sistemlerinde yapılan herhangi bir değişiklik, bilgiler ya da programları etkiler. Bunlar doğal riskle ilgili önemli risklerdir. Çünkü işletim sistemindeki bu tür bir zayıflık, yanlış yönetim bilgilendirmesine sebep olabilir (www.isaca.org 12.10.2022).

Kontrol Riski: Kontrol riski, kurumun iç kontrol yapısını yöneten politika, prosedürlerin önemli yanlış bildirimleri önleyememe ya da ortaya çıkaramama riskidir. Etkili olan iç kontrol yapısı kontrol riskini azaltabilirken zayıf olan iç kontrol yapısı kontrol riskini artırabilmektedir (www.isaca.org 12.10.2022).

Ortaya Çıkartma Riski: ISACA "*bilgi sistemleri denetim çalışmasında bilgi sistemleri denetim ve güvence uzmanlarının uyguladığı prosedürlerin var olan hatayı bulamama riski*" ni ortaya çıkartma riski olarak açıklamaktadır. Örneğin, bir uygulama sisteminin güvenlik açıklarını ortaya çıkaramama riski genellikle çok yüksektir. Çünkü inceleme sırasında inceleme sürecinin kayıt geçmişi mevcut olmayabilir (www.isaca.org 12.10.2022).

2.1.7. Bilgi Sistemleri Denetimi Kapsamında Kabul Görmüş Otoriteler

Günümüzde yaşanan teknolojik gelişmeler neticesinde denetim mesleği ve uygulamalarında değişiklikler kaçınılmaz olmuştur. Bu değişim neticesinde standartlar oluşturulmuş, yasal düzenlemeler yapılmıştır. Bu standartlar, denetim sürecinin geliştirilmesi için gereklilikleri düzenleyen çerçeveyi oluşturur. Ayrıca bu denetimi yapacak denetçilerin sorumlulukları ile denetçilerin yeterli bilgi ve tecrübeye sahip, dürüst, tarafsız, bağımsız olması gerekliliğini de belirtmektedir (Bilgin, Marmara Üniversitesi, 2016:57).

2.1.7.1. Uluslararası Otoriteler ve Düzenlemeleri

Bilgi sistemleri denetimi alanında uluslararası seviyede genel kabul görmüş 5 kuruluş bulunmaktadır. Bunlar Uluslararası Sayıştaylar Birliği, Uluslararası

Muhasebeciler Federasyonu, Amerikan Sertifikalı Muhasebeciler Enstitüsü, Uluslararası İç Denetçiler Enstitüsü, Bilgi Sistemleri Denetim ve Kontrol Derneği'dir.

2.1.7.1.1. Uluslararası Sayıştaylar Birliği (INTOSAI)

Uluslararası Sayıştaylar Birliği (INTOSAI) Ülkemiz Sayıştay'ında üyesi olduğu uluslararası bir Yüksek Denetim Kurumları kuruluşudur. INTOSAI üye devletlerin Sayıştayları arasında denetim, usul, yöntem ve tekniklerde birlik ve uyumu sağlamak amacıyla kurulmuştur (Özekicioğlu, 2018:77). INTOSIA Denetim standartlarının amacı; Kamu sektörü denetimi için ortak bir dil sağlayan farklı denetim görev türlerini ve ilgili kavram setini tanımlamak, yürütülen denetimlerin kalitesini sağlamak ve kullanıcılar için denetim raporlarının güvenilirliğini güçlendirmektir. INTOSIA standartlarına göre, muhasebe ya da bilgi sistemlerinin bilgisayarlaştırıldığı ortamlarda denetçinin birincil görevi, denetlenen kuruma ait verilerin doğruluğunu, eksiksizliğini ve güvenilirliğini sağlayan iç kontrollerin sağlıklı çalışıp çalışmadığını belirlemektir.

2.1.7.1.2. Uluslararası Muhasebeciler Federasyonu (IFAC)

Uluslararası Muhasebeciler Federasyonu (IFAC) muhasebe alanındaki en büyük küresel meslek kuruluşudur. Bu kuruluş denetim üzerine getirdiği standartlar ve Uluslararası Denetim Standartları ile bunların sürekli olarak geliştirilmesiyle ilgili olarak faaliyet göstermektedir. Bu kuruluş, denetim ile ilgili standartları, uluslararası denetim standartları ve bunların sürekli gelişimi ile ilgili faaliyet göstermektedir.

IFAC tarafından yayınlanan ISA bilgi sistemleri denetimi ile ilgili kontroller; ISA 300, ISA 315, ISA 330 ve ISA 402 standartları ile ifade edilmiştir. Belirtilen standartlarda, mali denetimlerde bilgi sistemleri uzmanı olan kişilerin görevlendirilmesi; otomatik kontrollerin değerlendirilmesi, genel denetim metodolojisinin oluşturulmasında bilgi sistemleri yapısındaki değişikliklerin de dikkate alınmasının gerektiği üzerinde durulmaktadır (KPMG "BT Denetim Standartları ve Uygulamaları", 2017).

2.1.7.1.3. Amerikan Sertifikalı Muhasebeciler Enstitüsü (AICPA)

Amerikan Yeminli Mali Müşavirler Enstitüsü (AICPA), ABD’de sertifikalı mali müşavirleri (CPA) temsil eden, kâr amacı gütmeyen bir profesyonel kuruluştur (<https://tr.nesrakonk.ru> 15.10.2010).

Ulusal meslek örgütü olan AICPA, denetim faaliyetlerinin yürütülmesinde belirleyici bir rol oynamaktadır. Kuruluş, meslek için etik standartlar ve özel şirketler, kâr amacı gütmeyen kuruluşlar, federal, eyalet ve yerel hükümetlerin denetimleri için ABD denetim standartlarını belirler. AICPA bünyesindeki Denetim Standartları Kurulu ilgili standartları yayınlamakta olup yayınlanan standartlara SAS adı verilmektedir. 1996 yılı aralık ayında yayınlanan SAS No: 80 (Kanıt Niteliği Taşıma), elektronik kanıtların geçerliliği, eksiksizliği ve bütünlüğü hakkındaki soruları yanıtlar. AICPA’nın yayımladığı 94 no.lu “*Bilgi Teknolojisinin Yasal Denetimlerde Denetçinin İç Kontrol Değerlendirmesine Etkisi*” standardı, elektronik bilgi işlem sistemlerinin bir şirketin iç kontrol sistemlerini nasıl etkilediğini açıklamaktadır. Ayrıca kontrol sistemi, iç kontrol sistemlerinin anlaşılmasına ve bu ortamlardaki kontrol riskinin değerlendirilmesine rehberlik etmektedir (Bilgin, 2016:59).

2.1.7.1.4. Uluslararası İç Denetçiler Enstitüsü (IIA)

“İç Denetçiler Enstitüsü (IIA), ulusal ve uluslararası otoriteler tarafından kabul edilmiş, iç denetim mesleği için savunuculuk yapan, eğitim konferansları sağlayan ve standartlar, rehberlik ve sertifikalar geliştiren bir kuruluştur. Üyeleri iç denetim, risk yönetimi, bilgi teknolojileri denetimi ve yönetim konularında uzman olan kişilerden oluşur.”

IIA tarafından yayınlanan, Uygulama Standartlarında iç denetçinin özelliklerinden biri olan yeterlilikle ilgili açıklamalarda *“iç denetçiler için tanımlanan görevi yerine getirmek için bilgi sistemleri ve kontrolleri ile alakalı önemli bilgilere ve mevcut teknoloji tabanlı denetim tekniklerine sahip olmaları gerektiği ancak, tüm iç denetçilerin, asıl sorumluluğunun bilgi sistemleri denetimi olan denetçiler kadar uzmanlığa sahip olması beklenmediği”* belirtilmektedir (Bilgin, 2016:59).

2.1.7.1.5. Bilgi Sistemleri Denetim ve Kontrol Derneđi (ISACA-Information Systems Audit and Control Association)

1969'da kurulan ISACA, bugün önde gelen BT yönetim, güvence, güvenlik ve kontrol profesyonel birliđidir. ISACA IS güvencesi, bilgi güvenliđi, kurumsal yönetim, BT risk yönetimi ve uyumluluk gibi alanlarda bilgi ve eğitim sağlamaktadır. CISA, CISM, Certified in the Governance of Enterprise IT (CGEIT) ve Certified in Risk and CRISC gibi dünya çapında bilinen sertifikalar/tanımlar sunmaktadır. COBIT standardı gibi uluslararası bilgi sistem denetim ve kontrol standartlarını geliştirmekte ve sık sık güncellemektedir. COBIT, hem bilgi sistemleri denetçilerine hem de bilgi teknolojileri yönetimine, güvence, güvenlik, risk ve kontrol alanlarında günlük görev ve sorumluluklarını yerine getirmelerinde yardımcı olmakta ve işe değer katmaktadır (Angel, 2018:168).

ISACA dünya genelinde farklı sektör ve seviyelerde çalışan 165.000' den fazla, uzman kişilerden oluşan üyelere sahiptir. Bu profesyoneller 180'den fazla ülkede BS/IT Denetimi, Risk, Güvenlik, Yönetişim, Eğitmciler, Danışmanlar ve Düzenleyiciler dahil olmak üzere çeşitli BT rollerinde çalışmaktadırlar. Bu çeşitlilik, üyelerin birbirlerinden öğrenmelerine ve çeşitli teknik konularda farklı bakış açılarını paylaşmalarına olanak tanımaktadır (www.isaca.org 17.10.2022).

2.1.8. ISACA Tarafından Yayımlanan Standartlar

2.1.8.1. COBIT (Bilgi ve İlgili Teknoloji için Kontrol Hedefler)

COBIT, Bilgi ve İlgili Teknoloji için Kontrol Hedefleri anlamına gelir. ISACA (Bilgi Sistemleri Denetim ve Kontrol Derneđi) tarafından oluşturulmuş bir çerçevedir. Yöneticiler için destekleyici bir araç olarak tasarlanmıştır ve teknik sorunlar, iş riskleri ve kontrol gereklilikleri arasındaki kritik boşlukta köprü kurulmasına olanak tanır. Genel olarak, COBIT bir organizasyondaki bilgi sistemlerinin kalitesini, kontrolünü ve güvenilirliğini sağlar (https://www.simplilearn.com 10.08.2022).

COBIT kurumsal hedeflere ulaşmak için amaca yönelik bilgi sistemlerinin kurulması ve kesintisiz, sürdürülebilir operasyonlar ve iş süreçlerinin kontrolü için gelişmiş bir kontrol çerçevesi sağlar. Kurumun iş ihtiyaçlarına ve genel kabul görmüş

süreçlere göre bilgi sistemini düzenler, bilgi sisteminin temel kaynaklarını belirler ve yönetim kontrol amaçlarını tanımlar. COBIT sadece bir denetim aracı değil, aynı zamanda bir bilgi teknolojileri yönetim aracıdır. İş gereksinimleri, bilgi sistemi kaynakları ve bilgi sistemi süreçleri olmak üzere temel olarak üç unsurdan oluşur (Drljača, D., Latinović B. 2016: 80).

COBIT, bilgi sistemleri denetçilerinin, yöneticilerinin güvene dayalı sorumluluklarını yerine getirmelerine, bilgi sistemlerini anlamalarına ve hangi düzeyde güvenlik ve kontrolün yeterli olduğuna karar vermelerine yardımcı olan kapsamlı bir kontrol hedefleri çerçevesidir. Barındırdığı 34 (otuzdört) süreç ile neredeyse gerekli tüm bilgi sistemleri işlevlerini kapsar. COBIT ayrıca, bilgi sistemlerinin maruz kaldığı riskleri, bu riskleri değerlendirecek, yönetecek ve ortadan kaldıracak kontrolleri ve bu kontrollerin nasıl denetlendiğini ele alan bir bakış açısıyla oluşturulmuş bir yapıya sahiptir (Drljača, D., Latinović B. 2016: 81).

2.1.8.2. ISO 27001/27002 Bilgi Güvenliği Yönetim Sistemi

ISO/IEC 27001, bilgi güvenliğinin nasıl yönetileceğine dair uluslararası bir standarttır. Standart ilk olarak Uluslararası Standardizasyon Örgütü (ISO) ve Uluslararası Elektroteknik Komisyonu (IEC) tarafından 2005 yılında ortaklaşa yayınlanmış ve ardından 2013, 2017, 2022 yıllarında revize edilmiştir (www.itgovernance.co.uk. 18.08.2022).

ISO/IEC 27001, bilgi güvenliği risklerinin yönetimiyle ilgili bir dizi faaliyetler paketi olan bir Bilgi Güvenliği Yönetim Sistemini (BGYS) resmi olarak tanımlar. BGYS, kuruluşların bilgi güvenliği risklerini tanımlamak, analiz etmek için kullandıkları çok yönlü bir yönetim çerçevesidir. Bir BGYS ile değişen güvenlik tehditlerini, güvenlik açıklarını ve iş etkilerini karşılamak için güvenlik düzenlemelerine katkı sağlar. Standart çok geniş kapsamlıdır ve tüm işletme türlerini kapsar (https://adeo.com.tr 12.08.2022).

ISO 27001'e göre bilginin aşağıdaki niteliklerinin korunması gerekmektedir. Şekil 2.7'de bu durum verilmiştir.

Şekil 2.7: Veri İşleme Süreci (KPGM BT Denetim Standartları ve Uygulamaları Araştırma Raporu 2017:22).



Gizlilik, bütünlük, erişilebilirlik bir işletmede kullanılan verilerin niteliklerinin korunması açısından önemlidir.

Gizlilik; bilginin yalnızca ona erişim izni olan kişiler tarafından erişilebilir olmasını sağlamak,

Bütünlük; bilginin ve nasıl işlendiğinin tam ve doğru olmasını sağlamak,

Erişilebilirlik; yetkili kullanıcılara, mevcut bilgilere ve ilgili varlıklara talep üzerine erişimi sağlamak,

olarak ifade edilebilir. Bu üç özelliğin yerinde olmasını sağlayan kontroller, işletmenin ihtiyaçlarına göre kurulmalıdır.

“ISO 27002 Bilgi Güvenliği Yönetim Sistemi için Uygulama Kodları Standardı ISO 27000 Bilgi Güvenliği Yönetim Sistemi standartlar ailesinin ikinci önemli standardı olup ISO 27001 Bilgi Güvenliği Yönetim Sistemi ne göre istem kurmuş firmaların performanslarını arttırmak için uyguladıkları bir standarttır.” ISO 27002 standardının amaçları; risk değerlendirmesi, güvenlik politikası oluşturma, varlık yönetimi oluşturma, fiziksel ve çevresel güvenliğin sağlanması, erişim kontrollerinin denetimi, iş sürekliliği prosedür ya da planlarını hazırlama vb. olarak sıralanabilir (kpmg.com.tr 24.08.2022).

2.1.8.3. ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi)

ITIL (Bilgi Teknolojileri Altyapı Kütüphanesi), bilgi sistemleri çalışanlarının verimliliğini arttırmak, insan hatasını en aza indirmek ve bilgi sistemlerinden yararlanan kullanıcıların memnuniyetini arttırmak için en iyi uygulamaları kapsayan bir doküman

kütüphanesidir. Diğer bir deyişle bilgi sistemi hizmetlerinin eksiksiz ve kaliteli yönetimi için hazırlanan hizmet yönetimi metodolojisidir (Akdaş, 2019:3).

ITIL, bilgi sistemleri için servis yönetimi ve dağıtım süreçleriyle küresel bir standarttır. ITIL, üst düzey bilgi teknolojisi hizmetleri sunmak için kullanılabilir sekiz kitaptan oluşur. Bu sekiz kaynaktan ikisi ön plandadır. Bunlar hizmet desteği, hizmet sunumudur (Meral, 2016:25). ITIL'in uygulanmasındaki amaç; bilgi sistemleri çalışanlarının memnuniyetini arttırmak, bilgi sistemleri hizmetlerinin erişilebilirliğini sağlamak, son kullanıcılara iyi bir hizmet sunabilmek, işletme kapasitesini ayarlamak, maliyetleri düşürmektir (Koç vd., 2019:131).

2.1.9. Ulusal Otoritelerin Düzenlemeleri ve Standartları

Türkiye'de kamu kurumlarında bilgi sistemleri kullanımı ve bilgi sistemleri ile ilgili işlemlerin yapılması yaygın olmaya başlamış ve denetim faaliyetleri kapsamında bilgi sistemlerinin test edilmesi zorunlu hale gelmiştir. Sayıştay, Bankacılık Düzenleme ve Denetim Kurumu, Gelir İdaresi Başkanlığı, Kamu Gözetim Muhasebe ve Denetim Standartları Kurumu, Sermaye Piyasası Kurulu bu alandaki önemli otoritelerdir.

2.1.9.1. Sayıştay

Sayıştay, kamu idarelerinin mali denetimini Türkiye Büyük Millet Meclisi adına yapan ve Türkiye'de bilgi işlem birimi kuran ilk kurumlardan biridir. Kamuda Vedop, Say2000i, Medula, e-Devlet, e-Teftiş gibi bilgi sistemlerinin kullanılmasıyla birlikte bilgi sistemleri denetlenmesine yönelik çalışmalar başlamıştır. Sayıştay tarafından 2013 yılının haziran ayında "*Bilgi Sistemleri Denetim Rehberi*" yayımlanmıştır. Sayıştay Bilgi Sistemleri Denetim metodolojisi, risk bazlı denetim yaklaşımına uygun bir çerçeve izler. Öncelikle riskler belirlenir, riskleri en aza indirmek için kontrol mekanizmaları oluşturulur, bu kontrol mekanizmalarının etkin bir şekilde çalışıp çalışmadığı, denetim sonucunda iç kontrollerdeki zafiyetler değerlendirilir ve raporlara yansıtılır (Bilgin, 2016:23).

2.1.9.2. Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)

Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) Türkiye'de finansal piyasalarda güven ve istikrarı sağlama, etkin şekilde işleyen kredi sistemini sürdürme, mali sektörün gelişmesini sağlama ve tasarruf sahiplerinin hak ve menfaatlerini koruma gibi çeşitli görevler yüklenmiş bir kamu kurumudur (Acuner 2017:57).

BDDK' nın bilgi sistemleri denetimiyle alakalı düzenleme ve uygulamalar yayımlaması ile bağımsız denetim kuruluşları için farklı bir dönem başlamıştır. BDDK tarafından 16 Mayıs 2006 tarihli ve 26170 sayı numaralı Resmi Gazete'de yayımlanan, *"Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik"* ile bilgi sistemleri denetimi *"denetlenenlerin faaliyetlerini gerçekleştirmekte kullandıkları yazılım ve donanım gibi tüm bilgi sistemi unsurlarının, bilgi sistemi süreçlerinin, finansal veri üretiminde kullanılan bilgi sistemi ve süreçlerinin ve bunlarla ilgili olarak tesis edilen iç kontrollerin nitelik, işleyiş, yeterlilik, bütünlük, güvenlik ve güvenilirliklerinin değerlendirilmesi ve rapora bağlanması aşamalarından oluşan, esas ve usulleri sözleşme ile belirlenen süreci"* şeklinde tanımlanmıştır.

Bankaların bilgi sistemleri ile finansal veri üretimine ilişkin süreç ve sistemlerinin, yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmesiyle ilgili usul ve esasları düzenlemek amacıyla yayımlanan *"Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik"* 13.Ocak.2010 tarihinde 27461 sayılı Resmî Gazete 'de yayımlanmıştır. Bankaların kullandıkları bilgi sistemlerinin yönetimi ile ilgili pek çok yayımlanan tebliğ ve yönetmeliğin (düzenlenmenin) ardından son olarak 31/12/2021 tarihli ve 31706 mükerrer sayılı Resmî Gazete'de yayımlanan *"Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Rapor Hakkında Tebliğ"* yayımlanmıştır. Bu tebliğ ile bağımsız denetim raporunun içerik, şekline dair usul ve esaslar belirlenmiştir. Bu yönetmelik ile yapılan değişiklikler;

- *"Bilgi sistemleri denetiminde COBIT referansı kaldırılmış yerine BSEBY' ye referans verilmesi,*
- *Finansal kiralama, Faktoring ve Finansman Şirketlerinde bilgi sistemleri denetimi sürecinin BSD Yönetmeliğine dâhil edilmesi,*

- *KGK tarafından kamu yararını ilgilendiren kuruluşlarda denetim yapma yetkisi verilen kuruluşlara, BDDK gözetimi ve denetimine tabi banka dışı kuruluşlarda bilgi sistemleri bağımsız denetimi yapma yetkisinin verilmesi,*
- *Bilgi sistemleri bağımsız denetim kuruluşları ve denetçiler izin sicil uygulamasının getirilmesi,*
- *Bilgi sistemleri bağımsız denetim kuruluşlarına veri güvenliği hakkında yeni yükümlülükler getirilmesi,*
- *Bağımsız denetim terminolojinin standardizasyonunun sağlanması kapsamında mümkün olduğu durumlarda KGK tarafından yayımlanan standartlara referans verilmesi”, şeklindedir.*

2.1.9.3. Gelir İdaresi Başkanlığı

Gelir İdaresi Başkanlığı vergiler ile diğer gelirleri tahsil etmekle sorumlu olan, Türkiye Cumhuriyetine bağlı olan devlet kurumudur. Ülkemizde tüm kamu kurumlarının iş süreçlerine uyarlanan dijital dönüşüm kapsamında GİB’in belirlediği standartlara uygun olarak elektronik ortamda oluşturulabilen belgelerin tamamı, e belge olarak tanımlanmaktadır.

19.11.2019 tarihinde Hazine ve Maliye Bakanlığı-Gelir İdaresi Başkanlığı tarafından “*e-Belge Özel Entegratörleri Bilgi Sistemleri Denetimi Kılavuzu*” yayınlanmıştır. Yayınlanan kılavuzda e-Belge entegratörlerinin faaliyetlerini gerçekleştirmede kullandıkları bilgi sistemlerinin yönetimi ile yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmelerine ilişkin usul ve esasları içeren bilgiler yer almaktadır.

2.1.9.4. Kamu Gözetim Muhasebe ve Denetim Standartları Kurumu

Kamu Gözetim Kurumu (KGK), denetim raporlarının doğru, bağımsız olarak hazırlanmasında ve güvenilir, anlaşılabilir, karşılaştırılabilir, finansal bilgilerin sağlanmasında yatırımcıların çıkarlarını ve kamu yararını korumayı amaçlayan bir kurumdur. Bu amaç doğrultusunda KGK uluslararası standartlar ile uyumlu Türkiye Muhasebe Standartlarını oluşturur ve yayımlar. Bağımsız denetimde güven ve kalite

sağlamak üzere denetim standartları belirler. Ayrıca bağımsız denetçi ve bağımsız denetim kuruluşlarını yetkilendirme görevi de bu kuruluşa aittir. Pek çok görev tanımlı olan KGK, 660 sayılı Kanun Hükmünde Kararname Madde 9 c bendi "*Finansal tabloların; işletmelerin finansal durumunu, performansını ve nakit akışlarını Türkiye Muhasebe Standartları doğrultusunda gerçeğe uygun olarak sunumunu, kullanıcıların ihtiyaçlarına uygunluğunu, güvenilirliğini, şeffaflığını, karşılaştırılabilirliğini ve anlaşılabilirliğini sağlamak amacıyla, kamu yararını da gözetmek suretiyle, bilgi sistemleri denetimi dahil, uluslararası standartlarla uyumlu ulusal denetim standartlarını oluşturmak ve yayımlamak.*" şeklindedir.

Bilgi sistemlerine ilişkin denetim standartları hazırlama görev ve yetkisi 660 Sayılı Yönetmelik ile KGK'ya verilmiştir. KGK tarafından 26.12.2012 tarih ve 28509 sayılı Resmî Gazete 'de yayımlanan Bağımsız Denetim Yönetmeliği'ndeki "*Denetim Kuruluşları ve Denetçilerin Yükümlülüklerini içeren 27.maddesine göre, bağımsız denetim süreci içerisinde denetim ekipleri, gerektirdiği sayı ve nitelikte denetçiden oluşabilmektedir. Denetim ekiplerinde; söz konusu denetim için yetkisi bulunmayan denetçiler, denetçi yardımcıları, bilgi sistemleri denetimi de dahil olmak üzere teknik bilgisine başvurulacak uzmanlar ve denetime yardımcı diğer kişiler de denetçi olarak görevlendirilmemek kaydıyla yer alabilir.*" Bu yönetmelik finansal denetim dahilinde bilgi sistemleri denetiminin de gerçekleştirileceği ve yeterli donanıma haiz denetçi yardımcılarının denetim ekibi içerisinde yer alabileceğine değinmiştir.

2.1.9.5. Sermaye Piyasası Kurulu (SPK)

Sermaye piyasası kurulu kamu kurumu olup, Türkiye'deki bütün menkul kıymetler piyasalarının düzenlenmesi, gözetiminin yapılması, denetlenmesi ve lisans verme yetkisi olan tek kuruluştur. Tasarruf sahiplerinin haklarının korunmasını sağlamak için düzenleme ve denetleme faaliyetlerini gerçekleştirmektedir.

Sermaye Piyasası Kurulu, Sermaye Piyasalarında Bağımsız Denetim Standartları Hakkında Tebliğ (Seri: X No:22)' in Onuncu Kısım İkinci Bölümde yer alan (madde 14)'te bilgi sistemleri ortamında yer alan iç kontrollere değinilmektedir. Bu madde "*İç kontrol sistemi ile ilgili risklerin yapısı ve kapsamı, işletmenin bilgi sistemlerinin yapısı ve özelliklerine göre değişir. Bu nedenle, bağımsız denetçi iç kontrol sistemini*

değerlendirirken, iç kontrol sisteminde bilişim teknolojilerinin ya da manüel olarak yapılan işlemlerin kullanılmasından kaynaklanabilecek risklerin ortaya çıkarmak ve gerekli tedbirleri almak üzere işletmenin etkili kontroller yapıp yapmadığını dikkate almak zorundadır" olarak belirtilmektedir.

Kurum, Kuruluş ve Ortaklıkların bilgi sistemlerinin yönetimi ve bağımsız denetimine ilişkin usul ve esasların belirlenmesi amacıyla 05.01.2018 tarihinde Sermaye Piyasası Kurulu tarafından “*Bilgi Sistemleri Yönetimi Tebliği*” ve “*Bilgi Sistemleri Bağımsız Denetim Tebliği*” Resmî Gazete ’de yayımlanmıştır.

Yayımlanmış olan mevzuatta yükümlülük sahibi kuruluşların denetçileri ile düzenleyecekleri sözleşmelere, bilgi sistemleri denetiminin kapsamına, sızma testi ve yönetim beyanına dair bilgiler yer almaktadır (<https://home.kpmg/tr/> 18.08.2022).

2.2. Bilgi Sistemleri Denetimi ve e-Belge Özel Entegratör Bilgi Sistemleri Denetimi

2.2.1. Bilgi Sistemleri Denetimi

Günümüzde pek çok işletme, gelişen teknoloji ile birlikte iş süreçlerinde bilgi sistemlerinin kullanımını her geçen gün daha da artırmaktadır. Önceleri yüksek maliyetler nedeniyle sadece büyük işletmelerce kullanılan bilgisayarlar (bilgi sistemleri) artık azalan maliyetler, paket yazılımların yaygınlığı ve gerekliliklerden dolayı orta ölçekli hatta bazı küçük işletmelerde de kullanılmaktadır. Bilgi teknolojilerinin muhasebe sistemlerine girmesi, verilerin saklanma, alınma ve kontrol edilme biçimini değiştirmiştir. Artık işletmeler finansal işlemler ve tüm iş süreçlerinde bilgi sistemlerinden faydalandıkları için kullanılan teknolojilere özgü riskleri de dikkate almak zorundadırlar. Bu durum bilgi sistemleri denetiminin gerekliliğinin önemini ortaya koymuştur.

Bilgi sistemleri (IS) denetimi, bir kuruluşun bilgi teknolojisi (BT) altyapısına özgü kontrollerin incelenmesidir. Bir başka ifade ile denetim “*bilgi sistemleri yönetimi ve işletimi kapsamında yer alan faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ile bu sistem dâhilinde tesis edilen kontrollerin BSY Tebliğinde düzenlenen bilgi sistemleri yönetim ilkeleri doğrultusunda değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması aşamalarından oluşan süreçtir.*” (SPK madde 5 (1)).

Bilgi sistemleri denetimi ile bilgi sistemleri altyapısının ve süreçlerinin beklenen faydaları üretip üretmediği kontrol edilmektedir. Bu faydalar verimlilik, etkinlik ve güvenlik olarak değerlendirilebilir.

- Verimlilik, iş ihtiyaçlarının karşılanma yeteneğidir.
- Etkinlik, kaynakların etkili kullanılmasıdır.
- Güvenlik, bilgilerin gizliliğinin, bütünlüğünün ve devamlılığının yanı sıra güvenilirliğinin ve hukuka uygunluğunun korunmasıdır.

İşletme ihtiyaçlarını karşılamak için uygulama sistemlerinin yeterliliğini değerlendirmek, iç kontrollerin yeterliliğini değerlendirmek ve bu sistemler tarafından kontrol edilen varlıkların yeterince korunmasını sağlamak için bilgi sistemleri denetimine ihtiyaç vardır.

Bilgi Sistemleri Denetimi, Elektronik Veri İşlem (EDP) Denetimi olarak başlamış ve “Equity Funding Corporation (Sermaye Finansmanı Şirketi)” skandalı sonrası yaygınlaşmıştır. Şirket yönetimi daha yüksek kâr göstermek için muhasebe kayıtlarını manipüle etmiş ve bu hileden sonra hisse senedi fiyatları hızla yükselmiştir. 10 yıl boyunca bu durum devam etmiş, 1973 yılında açığa çıkmıştır. 90’lı yılların sonunda ise AT&T2 şirketinin bilgi sistemlerinin, yazılım hataları yüzünden çökmesi nedeniyle pek çok kredi kartı sahibi 18 saat boyunca fonlara ulaşamamış ve dünya çapında ticaret bu durumdan olumsuz etkilenmiştir. Yaşanan bu olay bilgi sistemleri denetimi gerekliliğini göstermiştir (Yalkın, 2011: 22).

2001 yılında başlayan tarihin en büyük denetim skandalı, Enron ile pek çok yatırımcının para kaybetmesi, iflas, işsizlik gibi durumlar ortaya çıkmıştır. Yaşanan skandallar sonrası ABD’de 2002 yılında çıkartılan Sarbanes-Oxley yasası, halka açık işletmeler ile denetim firmalarına düzenlemeler getirmiştir (Dinç ve Cengiz, 2014: 223).

2003 yılında ülkemizde ortaya çıkan “çifte kayıt olayı” sebebiyle BDDK. T. İmar Bankası T.A.Ş.’ye ait bankacılık işlemlerini yapma ve mevduat kabul etme iznini kaldırmış ve bu bankanın Tasarruf Mevduatı Sigorta Fonu’na (TMSF) devredilmesini gerçekleştirmiştir. Çifte kayıt “*defterlere kaydı gereken hesap ve işlemleri vergi matrahının azalması sonucunu doğuracak şekilde tamamen veya kısmen başka defter, belge ve diğer kayıt ortamlarına kaydetme*” olarak tanımlanmaktadır (<https://upaymm.com.tr/> 15.10.2022). Çifte kayıt olayı bilgi sistemleri denetiminin önemini herkesin bilmesi gerektiği gerçeğini göz önüne sermiştir (Özbilgin, 2003: 127).

Ülkemizde 16 Mayıs 2006 tarihli 26170 sayılı Resmi Gazete'de yayımlanan, “Bankalarda Bağımsız Denetim Kuruluşlarınca Gerçekleştirilecek Bilgi Sistemleri Denetimi Hakkında Yönetmelik” gereği bilgi sistemleri denetimi "*denetlenenlerin faaliyetlerini gerçekleştirmekte kullandıkları yazılım ve donanım gibi tüm bilgi sistemi unsurlarının, bilgi sistemi süreçlerinin, finansal veri üretiminde kullanılan bilgi sistemi ve süreçlerinin ve bunlarla ilgili olarak tesis edilen iç kontrollerin nitelik, işleyiş, yeterlilik, bütünlük, güvenlik ve güvenilirliklerinin değerlendirilmesi ve rapora bağlanması aşamalarından oluşan, esas ve usulleri sözleşme ile belirlenen süreci*" olarak ifade edilmiştir (Bilgin, 2016: 62). Türkiyede BDDK tarafından 7 tane bilgi sistemleri denetimini gerçekleştirmekle yetkilendirilen bağımsız denetim kuruluşu bulunmaktadır.

Bilgi sistemleri Denetim süreçleri “Planlama”, “Kontrollerin Değerlendirilmesi”, “Raporlama ve Takip” olmak üzere 3 aşamadan oluşur (Sayıştay, 2013: 2).

2.2.1.1. Bilgi Sistemleri Denetiminin Planlanması

Denetim planlama aşamasında, denetçinin kuruluşun organizasyonel yapısı, operasyonları, bilgi sistemleri riskleri hakkında bilgi edinmesi gerekmektedir. Edinilen bilgiler ile denetçi, tüm bilgi sistemleri kontrol ortamını değerlendirir ve bir ön risk değerlendirmesi gerçekleştirir. Değerlendirmenin sonuçları, incelemenin sonraki aşamalarında uygulanan prosedürlerin kapsamını belirlemeye yardımcı olur.

Bilgi sistemleri denetim ve güvence standartları, 5 No’lu standarda göre “*Denetçi, denetiminin hedeflerini karşılayacak bilgi sistemleri denetim kapsamını yürürlükteki kanun ve mesleki denetim standartlarıyla uyumlu olarak planlamalıdır. Bilgi sistemleri denetçisi risk bazlı bir denetim yaklaşımı geliştirmeli ve belgelendirmelidir*” (ISACA, 2010: 13). Denetçi denetimin amacını ve kapsamını tanımlamak için risk değerlendirmesi yapmalıdır.

Bilgi Sistemleri Denetim ve Güvence Standartları 11 No’lu Standarda göre “*Bilgi sistemleri denetçisi, bilgi sistemleri denetim planının tamamını geliştirmede ve bilgi sistemleri denetim kaynaklarının etkili dağıtımı için önceliklerin belirlenmesinde kullanılabilir uygun bir risk değerlendirme tekniği veya yaklaşımı kullanmalıdır. Bilgi sistemleri denetçisi, kişisel denetim planlamasında, denetlenen alanla ilgili riskleri tanımlamalı ve değerlendirmelidir*” (ISACA, 2010: 20).

Aşağıda, bir denetçinin bir denetim planı geliştirmek için riske dayalı bir yaklaşım için izleyeceği adımlar yer almaktadır (Sayana, 2002: 2):

- İşletmedeki bilgi sistemlerinin envanterini çıkartmak, kategorilere ayırmak,
- Hangi sistemlerin, kritik işlevler ya da varlıkları etkileyebileceğini belirlemek,
- Sistemleri hangi olası risklerin etkileyebileceğini ayrıca iş üzerindeki etkinin ciddiyetini değerlendirmek,
- Bu değerlendirmelere bağlı olarak denetim önceliğine, kaynaklarına, zaman çizelgesi ve sıklığına karar vermek.

Denetim planının başlaması için denetim amaçlarının açık bir biçimde ortaya koyulması gerekmektedir. Ancak denetim esnasında bu amaçlar daha detaylı belirtilebilir ya da değişikliğe uğrayabilir.

Planlama, denetçinin, denetlenecek olan kuruluşun bilgi sistemlerine dair kontrollerini değerlendirmek için, maddi kanıt toplama metotlarını belirlemeye yardımcı olur. Bilgi sistemleri denetimi esnasında elde edilen kanıtlarla; bilgi sistemlerinin amaç ve hedeflere göre etkin bir şekilde çalışıp çalışmadığı, bilgi varlıklarının gizliliği, bütünlüğü ve erişilebilirliğinin sağlanıp sağlanmadığı tespit edilmeye çalışılır (Güredin, E., ve Uyar, S. 2020: 300)

2.2.1.2. Bilgi Sistemleri Kontrollerinin Değerlendirilmesi

Planlama aşamasından sonra bilgi sistemleri kontrollerinin değerlendirilmesi yapılmalıdır. Bilgi sistemleri kontrolleri incelemesi yapılırken kontrol alanlarında olması gerekli kontrollerin varlığı belirlenmelidir. Bu belirlemenin yapılabilmesi için denetçiye işletme tarafından sunulan kontrol setleri esas alınarak ve yetkili kişilerle görüşülerek elde edilen belgeler, cevaplara göre kontrollerin varlığı ve kontrollerin maruz kalabileceği risklerin önlenmesine dair ayrıca kontrollerin olup olmadığı tespit edilmelidir. Kontrol varlığının belirlenmesinin ardından kontrol etkinliğinin değerlendirilmesi gerekmektedir. Denetçi, yapılan bu değerlendirmenin ardından tespit edilen kontrol eksikliklerini kanıtlarla belgelemelidir. Denetçi bu konuda desteğe ihtiyaç duyarsa bir uzmandan yardım alabilir. Son olarak elde edilen bulgular değerlendirilir. Denetçinin tespit ettiği kontrol eksikliği ya da kontrol zayıflığı varsa bunlar bulgudur. Bulgular bilgi sistemlerine dair riskler içerir. Bu nedenle her kontrole dair bulguların risk seviyeleri belirlenmelidir.

Risklerin gerçekleşme olasılığıyla riskin etki seviyesi bir arada değerlendirilmelidir. Denetçi tarafından yapılan denetimler sonucunda elde edilen bulgular, denetimin sonucunu etkileyen yeterli delilin elde edilip edilmediği ve daha fazla araştırmaya gerek olup olmadığına göre değerlendirilmelidir. Daha fazla araştırmaya gerek duyulması halinde denetçi, denetim sürecini tamamlamadan önce ek kontroller yapmalıdır. Bilgi sistemleri kontrollerinin değerlendirilmesi genel ve uygulama kontrolleri olarak iki kategoride sınıflandırılabilir.

Genel Kontroller: Bir kuruluşun tüm bilgi sistemleri altyapısı ve destek hizmetleri de dahil olmak üzere iş sürekliliğini sağlayan politikalar, prosedürler ve uygulamalara dair kontroller genel kontrolleri oluşturur. Genel kontroller şunları içerir:

- “*Yönetim Kontrolleri*
- *Fiziksel ve Çevresel Kontroller*
- *Ağ Yönetimi ve Güvenliği Kontrolleri*
- *Mantıksal Erişim Kontrolleri*
- *İşletim Kontrolleri*
- *Değişim Yönetimi Kontrolleri*
- *Acil Durum ve İş Sürekliliği Planlaması Kontrolleri (Sayıştay, 2013: 11).”*

Yönetim kontrolleri: Bilgi sistemlerinin doğru çalışmasını ve iş hedeflerini karşılamasını sağlamak için yönetim tarafından benimsenen üst düzey kontrollerdir. Yönetim güvenli ve yeterli bir bilgi sistemleri ortamını sağlayabilmek için uygun politika ve prosedürler oluşturur. Bilgi sistemleri denetçisinin amacı, denetlenen kuruluşun uyguladığı kontrollerin bilgi sistemleri faaliyetlerinin kontrol edilmesini sağlamak için yeterli olup olmadığını belirlemek olacaktır. İşletme yönetim kontrolleri

- Resmi Organizasyon Şeması ve İş Tanımı
- Belgelendirme ve Doküman Saklama Politikaları
- Yasal düzenlemelere uygunluk
- Güvenlik politikaları
- Varlık yönetimi
- Görevlerin ayrılığı vb. alanlarından oluşur.

Belirtilen kontroller denetçiye alt düzeydeki ayrıntılı kontrollerin varlık ve etkinliğine dair makul bir güvence sağlamaktadır (Sayıştay, 2013: 11).

Fiziksel ve çevresel kontroller: Bu kontrollerin amacı, bilgi sistemlerine yetkisiz erişimi, müdahaleyi önlemektir. Bu amaca ulaşmak için, bilgisayar donanım ve yazılımlarının içerdiği ve kontrol ettiği bilgilerin yetkisiz kullanıcılara karşı korunması gerekir. Bu amaçla fiziksel bariyerler kurularak olası risklerin önüne geçilebilir. Ayrıca yangın, su (gerçek su veya aşırı nem), deprem, elektrik dalgalanmaları veya elektrik kesintilerinden kaynaklanan çevresel hasarlara karşı korunmalıdır. İşletmenin bilgi güvenliği politikası, fiziksel ve çevresel risklerin dikkate alınmasını içermelidir (Sayıştay, 2013: 28).

Ağ yönetimi ve güvenliği kontrolleri: Bu kontrollerin amacı ağlardaki verilerin güvenliğini sağlamak için uygun kontrollerin olmasını ve ağın yetkisiz erişime karşı yeterince korunmasını sağlamaktır. Kontroller şunları içerebilir:

- Operatörler ve ağ yöneticileri arasında görev ayrılığı.
- Uzak ekipmanın prosedürleri ve yönetimi için sorumluluğun oluşturulması.
- Ağ kullanılabilirliği ve performansının izlenmesi.
- Sistem yanıt süresini ve arıza süresini ölçmek için raporlar ve yardımcı programlar olmalıdır.
- Bilgisayar ağına özel güvenlik kontrollerinin oluşturulması ve izlenmesi. (Sayıştay, 2013: 36).

Mantıksal erişim kontrolleri: Bu kontrollerin amacı, işletim sistemini, uygulama programlarının ve temel alınan veri dosyalarının yetkisiz erişimine, değiştirilmeye, açığa çıkarmaya ya da silmeye karşı korunmasını sağlamaktır. Mantıksal erişim kontrolleri hem kurulum hem de uygulama düzeyinde bulunabilir. Genel bilgi sistemleri ortamındaki kontroller işletim sistemine, sistem kaynaklarına ve uygulamalara erişimi kısıtlarken, uygulama seviyesi kontrolleri bireysel uygulamalar içindeki kullanıcı aktivitelerini kısıtlar (Sayıştay, 2013: 64).

İşletim kontrolleri: Bu kontrollerin amacı bilgi sistemlerinden beklenen faaliyetlerin sürekliliği, güvenliği sağlayacak bir biçimde gerçekleştirmesini sağlamaktır. (Sayıştay, 2013: 74). İşletim kontrolleri; işletim sistemi ve bilgisayar işlemleri kontrolleri ve veri tabanı güvenlik kontrolleri olarak alanlara göre incelenir. Bu kontrollerin yeterli seviyede kurulmamış olması ya da yanlış kurulmuş olması; sistem çökmesi, kaynak yetersizliği, işlemlerin zorlaşması vb. gibi risklere neden olabilir.

Değişim yönetimi kontrolleri: Sistemlerin yapması gerekeni yapmaya devam ettiğine ve kontrollerin amaçlandığı gibi çalışmaya devam ettiğine dair güvence elde edebilmek için değişim yönetimi kontrollerine ihtiyaç vardır. Değişim yönetimi kontrolleri ile amaçlanan sistem geliştirme üzerindeki tüm proje yönetimi ve kontrollerinin tatmin edici olmasını, kalıcı ve yeterli iç kontrol ve denetim izine sahip olmasını, sistem geliştirme kalitesinin artırılmasını, sistemin kullanıcıların ihtiyaçlarını karşılamasını ve işletmenin stratejik hedeflerini de desteklemesini sağlamaktır (Sayıştay, 2013: 87).

Acil durum ve iş sürekliliği planlaması kontrolleri: Bu kontrollerin amacı, bilgi sistemlerinin geçici ya da kalıcı bir şekilde kesintiye uğraması halinde işletmenin faaliyetlerine devam edebilmesi ve elindeki verileri işleme, kullanma ve koruma kabiliyetini kaybetmemesini sağlamaktır. Acil durum, deprem, yangın, fırtına, sel, bombalama, sabotaj, donanım ya da yazılım arızası, güç ve telekomünikasyon gibi öngörülebilir veya öngörülemeyen ya da dış etkenler nedeniyle bir kuruluşun normal işleyişini bozan herhangi bir şey olabilir. (Sayıştay, 2013: 99).

Uygulama Kontrolleri: *“Uygulama kontrolleri, bilgilerin sistemlere ya da programlara tam olarak, zamanında ve sadece bir kere girilmesini, bilgi-işlem ortamında tüm işlem ve süreçlerin istenilen sıra ve düzen içinde gerçekleşmesini, raporların tam ve güvenilir olarak üretilmesini, yetkili kişilere ulaştırılmasını ve uygun şekilde arşivlenmesini sağlayan kontrollerdir”* (Sayıştay, 2013: 107).

Denetçi uygulama kontrollerini değerlendirdiğinde, uygulamalarda gerekli olan kontroller test edilir ve uygulamaların güvenilirliği hakkında yeterli güvence sağlamak için kanıtlar toplanır.

Uygulama kontrolleri aşağıdaki başlıklar altında incelenebilir:

- Girdi Kontrolleri
- Veri Transfer Kontrolleri
- İşlem Kontrolleri
- Çıktı Kontrolleri

Girdi kontrolleri: Girdi kontrolünün amacı, prosedürlerin ve kontrollerin; verilerin orijinal, tam, daha önce işlenmemiş, doğru ve uygun şekilde yetkilendirilmiş olduğunu ve verilerin doğru ve tekrarlanmadan girildiğini makul şekilde garanti etmesini sağlamaktır. Bilgisayarlı sistemlerde en önemli hata veya dolandırıcılık kaynağı yanlış

veya hileli girdi olduğundan girdi kontrolü çok önemlidir. Bu kontroller, sistemin bütünlüğü için hayati öneme sahiptir (Yıldırım, 2017:33).

Veri transfer kontrolleri: Bu kontrollerin amacı, bilgi sistemleri arasında aktarılan bilgilerin eksiksiz, doğru ve zamanında olmasını sağlamaktır. Aktarılan veriler aktarım sırasında bozulabilir, kaybolabilir, çalınabilir veya değiştirilebilir. Ayrıca verinin gelmemesi ya da birkaç defa gönderilmesi gibi problemler olabilir. Bu tür risklerin önüne geçmek için manuel ya da otomatik kontroller oluşturularak sistemler arası veri aktarımının eksiksiz ve doğru olması sağlanmaktadır. Ayrıca veri aktarımından sorumlu personele rehberlik eden uygulama ve prosedürleri tanımlamak oldukça önemlidir (Yıldırım, 2017:33).

İşlem kontrolleri: Girdilerin ve oluşturulan verilerin eksiksiz ve doğru bir şekilde işlenmesini ve denetlenebilir olmasını sağlar. Bu kontrollerin yetersiz olması sonucu hatalı verilerin işlenmesi, bir denetim izinin kaybolması ya da işlemlerin kontrol edilememesi gibi sorunlar söz konusu olabilir. Bu tip sorunlar kapsamında işletme yönetimi işlemlerin doğru, zamanında yürütülmesini sağlamak için otomatik ve manuel kontrollerin oluşturulmasını sağlamalıdır (Yıldırım, 2017:34).

Çıktı kontrolleri: Çıktıların eksiksiz, doğru ve zamanında üretilmesini, doğru yere/ kişilere ulaşmasını, gizliliğinin korunmasını, ortaya çıkarılan hataların derinlemesine araştırılmasını sağlamak amacıyla yapılır. Bu kontrollerin yetersizliğinden dolayı eksik ve hatalı çıktılar, yetkisiz erişim ve elde edilen sonuçların kaydedilmemesi gibi sorunlar söz konusu olabilir. Bu sorunları azaltmak için, kurumun çıktıları elde etmek ve sürdürmek için yazılı bir prosedürü olmalı ve çıktılardaki hataları gözden geçirme ve kontrol etme süreçleri yetkili personel tarafından gerçekleştirilmelidir (Yıldırım, 2017:34).

2.2.1.3. Bilgi Sistemleri Denetim Sonuçlarının Raporlanması ve İzlenmesi

Bilgi Sistemleri Denetim ve Güvence Standartları 7 No'lu Standarda göre "*Bilgi sistemleri denetçisi, denetimin tamamlanması sonucunda uygun biçimde bir rapor hazırlamalıdır. Rapor kurumu, hedeflenen kitleyi ve sunum sınırlamalarını tanımlamalıdır. Denetim raporu, yürütülen denetim işinin kapsamını, hedeflerini, denetim dönemini ve zamanlamasını, doğasını ve sınırlarını ortaya koymalıdır. Bilgi*

sistemleri denetçisinin denetimle ilgili olarak bulgularını, sonuçlarını ve önerilerini, sahip olduğu çekincelerini, niteliklerini veya sınırlandırmalarını belirtmelidir. Bilgi sistemleri denetçisi, raporlanan sonuçları destekleyecek uygun ve yeterli denetim kanıtlarına sahip olmalıdır. Bilgi sistemleri denetçisi, raporunu bitirdiği zaman raporunu imzalamalı, tarih atmalı ve denetim yönetmeliği veya hizmet sözleşmesine göre sunulmalıdır” (ISACA, 2014: 15).

Detaylı ana rapor aşağıdaki gibi bölümler başlığı altında oluşturulmaktadır (Yıldırım, 2017: 35).

Rapor özeti: Denetçinin detaylı raporundan önce gelen ve en önemli bulgularla ilgili açıklamalarını ve önerilerini içeren bölümdür.

Giriş bölümü: Denetime konu işletme, incelemeyi gerçekleştiren bilgi sistemleri denetçileri, denetim kapsamı hakkında bilgilerin yer aldığı bölümdür.

Ana rapor gövdesi bölümü: Detaylı denetim bulgularının yer aldığı bölümdür.

Öneriler bölümü: Ortaya çıkarılan kontrol eksiklikleri ve bu eksikliklerden kaynaklanan riskleri azaltacak önerilerde bulunulan kısımdır.

2.2.2. e-Belge Özel Entegratör Bilgi Sistemleri Denetimi

Günümüzde elektronikleşmenin hızlı gelişimi ve buna bağlı çözümlerin artış göstermesi neredeyse tüm sektörlerde dijitalleşmeyi ön plana çıkarmaktadır. Ülkemizde de dijital dönüşüm kapsamında Maliye Bakanlığına bağlı, Gelir İdaresi Başkanlığı tarafından e-Fatura, e-Arşiv fatura, e-İrsaliye, e-Defter, e-Bilet, e-serbest meslek makbuzu (SMM), e-Müstahsil Makbuzu gibi uygulamaların tamamının e-belge başlığı altında hayata geçtiği görülmektedir. e-Belge; muhasebe alanında kullanılan belgelerin elektronik ortamda oluşturulup ibraz edilmesini sağlayan bir uygulamadır. Pek çok e-belge çeşidi bulunmakta olup hepsinin amacı farklıdır. Bahsi geçen elektronik belge çeşitlerinin kullanılabilmesi için sağlanması gereken şartlar farklılık göstermektedir. Bazı e belgeler istenilen kişilerce kullanılabilirken bazılarının kullanılması kimi gruplar için zorunludur (Durmuş, A.F., ve Koca, Z. 2019: 281).

Günümüzde kullanılmakta olan birden fazla elektronik belge çeşidi vardır. Dünyanın çeşitli ülkelerinde kullanılan, ülkemizde de elektronik ortamda işlenebilen,

ibraz edilebilen bu belgelerin sayısı sürekli artış göstermektedir. Ülkemizde mükellefler tarafından kullanılan elektronik belge türleri aşağıdaki gibidir.

e-fatura: Günümüzde yaygın bir biçimde kullanılan elektronik belgedir. Türkiye’de 397 Sıra No.lu Vergi Usul Kanunu Genel Tebliği ile hayata geçirilen ve 5 Mart 2010 tarihinden itibaren uygulamada olan e-Fatura, “*veri format ve standardı Gelir İdaresi Başkanlığı tarafından belirlenen, 213 sayılı Vergi Usul Kanunu hükümleri gereği bir faturada yer alması gereken bilgileri içeren, satıcı ve alıcı arasındaki iletiminin merkezi bir platform (GİB) üzerinden gerçekleştirildiği elektronik bir belgedir.*” GİB tarafından organize edilen e-Fatura uygulamasının amacı tek format ve standarda göre satıcı ile alıcı arasında güveni, zamandan ve maliyetten tasarrufu sağlayan sistem oluşturmaktır (Gülten ve Erdem 2021: 40).

e-Arşiv Fatura: E-arşiv fatura elektronik fatura uygulamasından farklı ve değişik bir mantıkla çalışan elektronik faturalaşma sisteminin adıdır. 509 nolu VUK tebliğinde e-arşiv fatura uygulaması “*VUK 509 Nolu tebliğin de yer alan şartlara uygun şekilde ve başkanlık tarafından belirlenen standartlara uygun olarak e-Arşiv Faturanın elektronik ortamda oluşturulması, elektronik ortamda muhafazası, ibrazı ve raporlamasını kapsayan uygulamayı*” tanımlar şeklinde açıklanmıştır (Gülten ve Erdem 2021: 88)

e-Serbest Meslek Makbuzu: Serbest Meslek Makbuzu belgesinin elektronik olarak oluşturulmuş, ibraz edilen biçimidir. SMM serbest meslek erbaplarının gelirini beyan ettiği ve vergi, denetim, kayıt için sunulan belgedir. e-Serbest Meslek Makbuzu ve ya e-SMM fiziksel SMM ile aynı statüdedir (Öner, 2022: 75)

e-İhracat Faturası: İhracat e-faturası, e-fatura uygulamasına kayıtlı olup, yurtdışına gümrük çıkış beyannamesi ile mal ihracatı yapanların düzenleyecekleri e-fatura türüdür. Şubat 2018 tarihli e-Fatura Uygulaması Gümrük İşlemleri Kılavuzu V.1,8’de “*İhracat faturalarının e-fatura olarak düzenlenmesi zorunluluğu sadece Gümrük Beyannamesi ekinde yer alan mal ihracı faturaları için geçerlidir. Diğer belgelerin (Serbest Bölge İşlem Formu, transit ticaret formu vb.) ekinde yer alan ihracat faturaları e-fatura kapsamında değildir*” açıklaması yer almaktadır (Gülten ve Erdem 2021: 58).

e-İrsaliye: Adından da anlaşılacağı üzere satış işlemi sonrasında hazırlanan irsaliye belgesinin elektronik türüdür. Elektronik irsaliye, fiziksel irsaliyenin tüm bilgilerini içerir

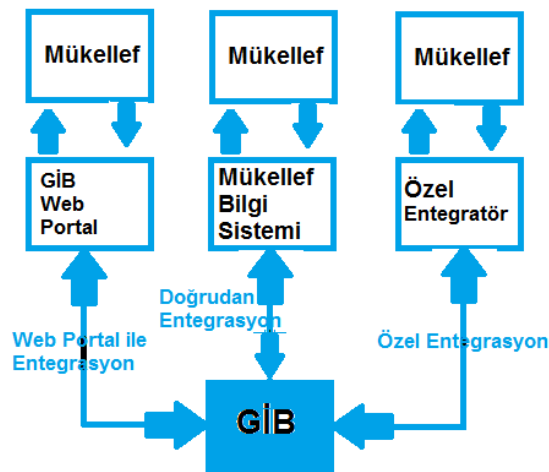
ve aynı statüye sahiptir. e-irsaliyeyi kullanmak için e-fatura kullanılması gerekmektedir (Öner, 2022: 73).

e-Defter: “Elektronik defter kanunen vergi mükelleflerinin tutmak zorunda oldukları ticari defterlerin önceden belirlenen standartlara ve formata uygun bir şekilde oluşturulduğu, kayıt edildiği elektronik imza veya mali mühür ile doğruluğunun ispat edildiği teknik ve hukuki sistemin tamamına verilen addır “ (Özer, 2015: 76).

e-Gider Pusulası: VUK 509 Nolu tebliğinde elektronik gider pusulası (e- gider pusulası) “VUK 509 Nolu tebliğinde yer alan şartlara uygun olarak elektronik belge biçiminde oluşturulmuş gider pusulasını” ifade eder şeklinde tanımlanmıştır. Gider pusulası, defter tutan işletmeler defter tutmayan işletmelerle satın alımlar gerçekleştirdiklerinde bunu belirtmek için kullanılır (Gülten ve Erdem 2021: 139).

Birçok maliyeti ortadan kaldıran elektronik belge türleri daha çok tercih edilmektedir. Fiziksel basılı belgeler yerine elektronik belge kullanılmasının avantajları vardır. Bu belgeler sayesinde muhasebe işlemleri, kontrol ve izleme işlemleri, vergilendirme daha kolay yapılabilmektedir. e-Belgelerin elektronik ortamda iletimi, GİB Web Portal, Doğrudan Entegrasyon veya Özel Entegrasyon ile sağlanabilmektedir. Şekil 2.8’ de gösterilen e-Belgelerin elektronik ortamda iletimi yöntemleri hakkında bilgiler aşağıda verilmiştir.

Şekil 2.8: e-Belgelerin elektronik ortamda iletimi yöntemleri (<https://home.kpmg/tr>)



Gib Web Portal yöntemi: VUK 509 Nolu tebliğinde GİB Portalı (GİB e- Belge Portalı) “e-Fatura, e-Arşiv Fatura, e-İrsaliye, e-Serbest Meslek Makbuzu, e-Müstahsil

Makbuzu ve e-Gider Pusulası ve benzeri diğer e-Belge uygulamalarına ait temel fonksiyonların, internet üzerinden genel kullanımını sağlamak amacıyla başkanlık tarafından geliştirilen portalleri” ifade eder şeklinde tanımlanmıştır. Portal yöntemi ayda çok fazla e-belge düzenlemeyecek olan mükellefler için ideal ve ücretsiz bir yöntem olup bu yöntem için mükellefin çok ciddi bir bilişim alt yapısı oluşturması gerekmemektedir. İnternete bağlı bir bilgisayarın, tabletin veya akıllı cep telefonun olması yeterlidir.

Doğrudan Entegrasyon Yöntemi: VUK 509 Nolu tebliğinde doğrudan entegrasyon yöntemi, *“Kendi bilgi işlem sistemlerinin başkanlık bilgi işlem sistemleri ile doğrudan entegre edilmesi yolu”* olarak tanımlanmıştır.

Bazı işletmelerin her gün binlerce elektronik belge düzenlemesi gerekebilir. Bazı şirketler, bilgilerinin özel entegratörler gibi dış şirketlerle paylaşılmasını istemeyebilir. Bu gibi durumlarda mükellefler, elektronik belge uygulamalarına özel ihtiyaçlarına göre tasarlanmış bilgi işlem sistemlerini entegre etmek zorunda kalabilmektedir. Bu yöntem, çok fazla elektronik belge düzenleyen ve gerekli bilgi işlem yapısını oluşturmak için bazı maliyetler ödemeye razı olan mükellefler tarafından kullanılmaktadır. Entegrasyon alt yapısını kurmak için bakanlığın hazırladığı entegrasyon kılavuzlarından yararlanılması ve istenilen yapı ve standartlara uygun bir bilişim sistemi kurulması gerekmektedir.

Özel Entegrasyon Yöntemi: VUK 509 Nolu tebliğinde özel entegratör *“VUK 509 Nolu tebliğinde belirtilen elektronik belgelerin oluşturulması, imzalanması, iletilmesi hususlarında mükelleflere hizmet verme konusunda teknik yeterliğe sahip ve test ve değerlendirme süreçleri sonunda Başkanlıktan izin alabilen entegrasyon kuruluşlarını”* ifade eder şeklinde tanımlanmıştır.

E-belgelerin bu alanda uzman aracı (yazılımcı) firmaların sistemleri aracılığı ile gönderilmesine özel entegratör kullanımı denilmektedir. Özel entegratör kullanımı hem ülkemizde hem de yabancı uygulamalarda en popüler yöntem olarak bilinmektedir. Özel entegratörler, portal yönteminde kullanılan birçok manuel işlemi otomatikleştirerek, yazılımları ile e-belge süreçlerinin çok daha hızlı yönetilmesini sağlamaktadırlar. Bu özel entegratörler, aracı firmalar, yazılım firmaları veya servis sağlayıcılar olarak ta adlandırılmaktadırlar. Özel entegrasyon yöntemini seçen bir mükellef, elektronik belge verilerini özel entegratörün kullanıcı arayüzüne yükleyerek ve veri girişi yaparak aracı kurumlar vasıtasıyla elektronik belge gönderip alabilirler. Özel entegratörleri kullanan mükellefler, genellikle belirli bir süre içinde çok sayıda elektronik belge

düzenleyenlerdir. Yazılım endüstrisinde uzman olan bu uzman entegratörler, kullanıcı dostu arayüzler geliştirmekte ve e-belgelerin maliye bakanlığının sisteminden çok daha hızlı ve kolay bir şekilde gönderilip alınmasını sağlamaktadır. e-Belgelerin elektronik ortamda iletim yöntemlerinin karşılaştırılması Tablo 2.2’ de verilmiştir.

Tablo 2.2: e-Belgelerin elektronik ortamda iletim yöntemleri (Gülten, e-Maliye Muhasebe Uygulamaları Eğitim Notlarından alınmıştır. <http://www.esmmmo.org/>)

<u>ÖZEL ENTEGRATÖR YÖNTEMİYLE</u>	<u>ENTEGRASYON YÖNTEMİYLE</u>	<u>GİB PORTALI YÖNTEMİYLE</u>
➤ Mükellefin mali mühür alması zorunludur. Ancak yine de faturada entegratörün mali mührü kullanılabilir.	➤ Mali mühür almak zorunludur.	➤ Mali mühür almak zorunludur.
➤ Yüksek tutarlı IT yatırımı yapma gereği yoktur.	➤ Kullanılan muhasebe sistemine göre değişen yüksek tutarlı IT yatırım maliyeti gerekmektedir.	➤ Sadece 6 ay faturalar portalda saklanır.
➤ Entegrasyon işlemi son derece hızlı ve kolay olmaktadır.	➤ Entegrasyon süresi uzun zaman almaktadır.	➤ Az sayıda fatura alıp, gönderen küçük ölçekli firmalar için uygundur.
➤ Sisteme giriş maliyeti ekonomiktir ve bakım maliyeti yoktur.	➤ Faturaların yurt içinde arşivlenmesi zorunluluğu bulunmaktadır.	➤ Manuel fatura girişine uygundur.
➤ Olası mevzuat değişikliklerinde gerekli güncellemeleri entegratör ücretsiz yapacaktır.	➤ Olası mevzuat değişikliklerinde yazılımın güncellenmesi gerekmektedir.	➤ Arşivleme mükellefin sorumluluğundadır.
➤ Arşivleme ve iş sürekliliğine uygun altyapı entegratör tarafından yapılacaktır.	➤ İş sürekliliğine uyum için ekstra yatırım maliyeti doğmaktadır.	
➤ Çok sayıda kullanıcıya farklı yetkilerde sisteme giriş izni verilebilmektedir.	➤ 7/24 çalışır durumda olmak ve teknik arızalarda maksimum 48 saat içerisinde sorunun giderilmesi zorunluluğu bulunmaktadır.	

GİB Özel Entegrasyon izni alan akredite kuruluşlar, teknik yeterliliğe sahip bilgi işlem sistemi vasıtası ile e-fatura uygulamasına kayıtlı mükellefler ile kayıt olmak isteyen mükelleflere, e-fatura yazılım ve donanım altyapı uygulaması ile elektronik fatura gönderme ve alma hizmeti sunmaktadır. Bu doğrultuda söz konusu özel entegratörler GİB tarafından bilgi sistemleri denetimine tabi tutulmuştur.

GİB 19 Kasım 2019'da e-Belge entegratörlerinin faaliyetlerini gerçekleştirmede kullandıkları bilgi sistemlerinin yönetimi ile yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmelerine ilişkin usul ve esasları içeren e-Belge Özel Entegratörleri Bilgi Sistemleri Denetimi (ÖEBSD) Kılavuzu'nu yayınlamıştır.

Yapılan düzenlemeyle, yayımlandığı tarihinden sonra yapılan özel entegratörlük başvurularında, adayların kılavuzda ifade edilen Bilgi Sistemleri Denetimini yaptırmaları gerekmektedir. Ayrıca başvuru dosyasında “ÖEBSD Görüş Yazısı ve Raporu” da eklenmiş olmalıdır. İlk denetimin yapıldığı tarihten itibaren 2 yılda bir, BSDHY kapsamında yetki verilmiş ya da izin verilmiş olan bağımsız denetim kuruluşları tarafından bilgi sistemleri denetiminin yapılması ve GİB'e iletilmesi beklenmektedir.

Bilgi sistemleri yönetimi kapsamında yer alan süreç, faaliyet, yazılım ve donanım gibi bilgi sistemi unsurları ile bu sistem ve süreçler dâhilinde tesis edilen iç kontrollerin uyumluluk, etkinlik ve yeterliliklerinin değerlendirilmesi sonucunda görüş oluşturulması ve rapora bağlanması bu denetimin amaçlarını oluşturmaktadır. E-belge özel entegratörleri bilgi sistemleri denetimi aşağıdaki süreçlerden oluşur (ÖEBSD Kılavuzu 2019: 6)

2.2.2.1. Denetim ve Onay Süreci

Özel entegratör kuruluşlar, ilk denetim hariç olmak üzere, ilk denetim tarihinden itibaren 2 yılda bir GİB in yayınlamış olduğu kılavuzda belirtilen gereklilikler doğrultusunda bilgi sistemleri denetimi (ÖEBSD) yaptırmakla yükümlüdür. Hazırlanan bağımsız denetim raporu, rapor tarihinden itibaren 2 yıl geçerlidir. Süre bittikten sonra yeni bağımsız denetim raporunun GİB'e ibrazı zorunludur (ÖEBSD Kılavuzu 2019: 6).

Özel entegratör kuruluşları, denetim için belirlenen tarihten en az 1 ay önce güncellenmiş BİS raporunu, GİB'e ayrıca denetimi gerçekleştirecek kuruluşa gönderir. Denetim sonuçları, “ÖEBSD Görüş Yazısı ve Raporuyla” kayıt altına alınır. ÖEBSD'nin

sonucu raporun hazırlandığı tarihten hemen sonra en geç 15 günde GİB 'e yazılı olarak iletilir. Bağımsız denetçi olumlu görüş, olumsuz görüş, şartlı görüş bildirebilir. Hatta görüş bildirmekten de kaçınabilir. Denetim esnasında kısa zamanda tamamlanabilecek eksiklikler tespit edilmesi halinde rapora açık bir şekilde yazılır (ÖEBSD Kılavuzu 2019: 6).

ÖEBSD raporu verilen sürede başkanlığa ulaşmamış ise özel entegratörlerle özel entegratör adaylarının izinleri/başvuruları ilk olarak askıya alınır, ebelge.gib.gov.tr adresinden duyurulur. Raporların teslimi için 6 ay ek süre verilir. Bu ek sürenin geçmesine rağmen rapor teslim edilmezse özel entegratöre verilen faaliyet izni iptal edilir (ÖEBSD Kılavuzu 2019: 7).

Özel Entegratör Bilgi sistemleri Denetim süreçleri “Planlama”, “Kontrollerin Değerlendirilmesi”, “Raporlama” olmak üzere 3 aşamadan oluşur (Yıldırım, 2017: 24).

2.2.2.2. Denetimin Planlanması

Bilgi sistem denetçisinin denetim görüşüne ulaşmada temel olacak faaliyetlerin nasıl ve ne şekilde yürüteceği hakkındaki davranış düzenine denetim planlaması denir. Planlama, denetimin başında yoğunlaşılmasına rağmen, denetim boyunca gerçekleştirilen yinelemeli bir süreçtir. Bunun nedeni, ön değerlendirmelerin sonuçlarının, sonraki testlerin kapsamını ve türünü belirlemek için temel sağlamasıdır. Denetçiler, belirli kontrol prosedürlerinin etkisiz olduğuna dair kanıt elde ederse, daha önceki sonuçlarını ve bu sonuçlara dayalı olarak alınan diğer planlama kararlarını yeniden değerlendirmeyi gerekli görebilirler. Planlama aşamasında bilgi sistemleri denetçisi, denetlenecek kuruluşun aşağıdaki yönleri hakkında bilgi ve girdi toplamalıdır:

- Kuruma ait çeşitli iş uygulamaları ve işlevleri, faaliyeti destekleyen bilgi sistemleri türleri ve faaliyet gösterdiği ortam,
- Başarısızlığı örgüt üzerinde çok ciddi sorunlara neden olabilecek kritik görev sistemleri ve yönetimin karar almasını destekleyen destek sistemleri,
- Denetçinin ilgili riskleri anlayabilmesini sağlamak için kullanılan donanım ve yazılımın niteliği,
- Kullanılan ağ mimarisi, bağlantı kurma teknolojisi, güvenlik duvarlarının yerleştirildiği yerler vb.

- Sistemleri etkileyen risklerin niteliği ve kapsamı,
- Sistemleri etkileyen risklerin doğası ve kapsamı.

Denetçinin ön değerlendirme aşamasında elde edeceği bu bilgiler denetim yaklaşımının ve kanıt toplama için gerekli kaynakların planlanmasını sağlayacaktır. Denetçi bu bilgileri; gözlem, fiziki inceleme yaparak, kilit personelle görüşerek, önemli organizasyon tesislerini ziyaret ederek, yıllık raporları ve kuruluş yayınlarını inceleyerek vb. yollarla edinebilir (IT Audit Manual 2017:15-20).

Denetçinin ihtiyaç duyduğu kuruluş ve süreçleri hakkındaki bilginin kapsamı, kuruluşun niteliğine ve denetim çalışmasının yürütüldüğü ayrıntı düzeyine göre belirlenecektir. Kuruluşla ilgili bilgi, kuruluşun karşı karşıya olduğu ticari, finansal ve yapısal riskleri içermelidir. Ayrıca, kuruluşun hedeflerine ulaşmak için dış kaynak kullanımına ne ölçüde bağlı olduğunu da içermelidir. Denetçi, bu bilgileri potansiyel sorunları belirlemede ve çalışmanın amaçlarını ve kapsamını formüle etmede kullanılmalıdır (IT Audit Manual 2017:15-20).

2.2.2.3. Kontrollerin Değerlendirilmesi

e-Belge Özel Entegratör kuruluşunun bilgi sistemleri altyapısı ve destek hizmetleri de dahil olmak üzere iş sürekliliğini sağlayan politikalar, prosedürler ve uygulamalara dair kontroller genel kontrolleri oluşturur. Bilgi sistemleri kontrolleri incelemesi yapılırken, GİB tarafından yayınlanan kılavuzda yer alan kontrol alanlarında olması, gerekli kontrollerin varlığı bilgi sistem denetçisi tarafından belirlenmelidir. Bunun tespiti için denetçiye işletme tarafından sunulan kontrol setleri esas alınarak ve yetkili kişilerle görüşülerek elde edilen belgeler, cevaplara göre kontrollerin varlığı ve kontrollerin maruz kalabileceği risklerin önlenmesine dair ayrıca kontrollerin olup olmadığı tespit edilir. Aşağıda e Belge Özel Entegratör kuruluşları için GİB tarafından hazırlanmış kılavuzda yer alan kontrol grupları ve denetçinin denetimde kullandığı değerlendirme sınıfları hakkında bilgiler yer almaktadır.

2.2.2.3.1. Fiziki Güvenlik Şartları ve Tedbirleri

Fiziki güvenlik şartları ve tedbirlerinin amacı, bilgi sistemleri hizmetlerine yetkisiz erişimi, müdahaleyi önlemektir. Bunu sağlayabilmek için bilgisayar donanımı, içerdiği ve kontrol ettiği bilgiler yetkisiz kullanıcılardan korunmalıdır. Ayrıca yangın, su (aşırı nem), depremler, elektrik dalgalanmaları veya elektrik kesintilerinden kaynaklanan çevresel hasarlardan da korunmalıdırlar. Bilgi sistemleri alanında, hataların ikinci en önemli olası nedeni doğal afetlerdir. Kurumun bilgi sistemleri güvenlik politikası, fiziksel ve çevresel risklerin dikkate alınmasını içermelidir. Tablo 2.3’de fiziksel ve çevresel risk alanları belirtilmiştir (IT Audit Manual 2017:15).


Tablo 2.3: Fiziksel ve Çevresel Risk Alanları

Fiziksel Risk Alanları	Çevresel Risk Alanları
Personel tarafından kazara veya kasıtlı hasar	Yangın/su hasarı (veya diğer doğal afetlerden kaynaklanan hasarlar);
Bilgisayarların veya bileşenlerinin çalınması	Güç: Geçici depolamada (RAM) veri kaybına yol açan kesintiler
Bileşenlerin zarar görmesine ve verilerin kaybolmasına veya bozulmasına neden olabilecek güç artışları veya dalgalanmaları	Ani artışlar: sistem arızalarına, işleme hatalarına, ekipman bileşenlerinde hasara yol açar.
Mantıksal erişim kontrollerinin atlanması: örneğin bir dosya sunucusuna fiziksel erişime sahip olmak, parolalar gibi mantıksal kontrolleri atlamak için kullanılabilir.	Aşırı sıcaklık veya nem (veya birkaç derecelik toleransların hemen dışında) nedeniyle ekipmanın arızalanması;
Hassas veya gizli bilgilerin kopyalanması veya görüntülenmesi,	Statik elektrik: hassas elektrikli bileşenlere zarar verebilir. Bilgisayar çipleri (ROM, RAM ve işlemci) hassastır ve statik elektrik çarpmalarından kolayca zarar görebilir. Diğerleri:(örneğin şimşek çakması)

İşletmenin varlıklarını ve kaynaklarını korumak için yeterli iç kontrollerin mevcut olduğundan emin olmak için kuruluş bir risk değerlendirmesi yapmalıdır. Bu değerlendirme, sistemlere yönelik tehditlerin, sistem bileşenlerinin güvenlik açığının ve meydana gelen bir olayın olası etkisinin belirlenmesini içerecektir. Ardından, maruz kalma düzeyini kabul edilebilir bir düzeye indirmek için karşı önlemleri belirlemelidir. Bunu yapmak için, belirlenen riskleri kontrol uygulama maliyetiyle dengelemelidir. Fiziksel ve çevresel kontroller tablo 2.4’de görülmektedir (www.ms.hmb.gov.tr 22.08.2022)

Tablo 2.4: Fiziksel ve Çevresel Kontroller

Fiziksel Kontroller	Çevresel Kontroller
Fiziksel erişim kontrolleri, özellikle sadece yönetim tarafından yetkilendirilmiş kişilerin bilgisayar sistemlerine fiziksel erişiminin olmasını sağlamayı amaçlar. Fiziksel erişim güvenliği, bilgi sistemleri tesislerini çevreleyen belirlenmiş çevreler kavramına dayanmalıdır.	Bilgisayar kurulumları yangın, sel, elektrik kesintisi, fiziksel hasar ve hırsızlık gibi tehlikelere karşı korunmalıdır. Yetersiz koruma, sistem kullanılabilirliği riskini ve nihayetinde bir kuruluşun eksiksiz bir finansal işlem kaydı oluşturma yeteneğini artırır. Kuruluş, hasara maruz kalmayı değerlendirmeli ve riski kabul edilebilir bir düzeye indirmek için uygun kontrolleri uygulamaya koymalıdır.
Fiziksel erişim kontrolleri, yetkisiz kişilerin bilgisayar ekipmanına erişme riskini azaltır. Denetçi, kuruluşun sitesine, bilgisayar odalarına, terminallere, yazıcılara ve veri depolama ortamına erişimi kısıtlayacak kontrolleri belirlemelidir.	Yangın algılama ve yangınla mücadele ekipmanlarının sağlanmasıyla yangın hasarı riski azaltılabilir. Düzenli temizlik ve bilgisayar odasından atıkların uzaklaştırılması gibi diğer önlemler yangın hasarı riskini azaltacaktır.
Kuruluşun sahasına ve güvenli alanlara erişim, çevre çitinden başlayarak ve binanın girişinden bilgisayar odasına ve	Su hasarı riski büyük ölçüde bilgisayar tesislerinin konumuna bağlıdır. Boruların ve su depolarının yakınında bulunan

<p>terminallere kadar uzanan kontrol katmanları tarafından kontrol edilmelidir.</p>	<p>ekipmanlar yüksek risk altındadır. Mümkün olduğunda, kuruluşlar bilgisayar ekipmanlarını bodrum katlarına veya su depolarının hemen altına veya yakınlara yerleştirmekten kaçınmalıdır. Bilgi sistemleri personelini olası su girişine karşı uyarmak için otomatik nem dedektörleri kullanılabilir.</p>
	<p>Bilgisayar ekipmanı, elektrik güç kaynağındaki dalgalanmalardan zarar görebilir veya bozulabilir. Güç dalgalanmaları, bilgisayar sistemlerinin verileri silmesine veya kirlenmesine neden olabilir. Kesintisiz güç kaynakları, sistem kesintisi ve hasar riskini azaltır ve bir elektrik kesintisinden sonra işlemin devam etmesine izin verebilir.</p>

GİB tarafından hazırlanan kılavuza göre özel entegratörün bilgi sistemleri için aşağıdaki önlemleri alması gerekir (ÖEBSD Kılavuzu 2019: 9).

- *“Fiziki erişim imkânı*
- *Uygun iklimlendirme ortamını sağlamak*
- *Yangın, sel vb. doğal afetler için makul uyarı ve korunma tedbirleri almak*
- *Bilgi sistemlerinin çalıştığı tüm odalarda asgari ISO standartlarını sağlamak*

Özel entegratörün bilgi sistemlerinin tamamı veya bir bölümü için dışarıdan hizmet alması halinde de sayılan tedbirlerin alınması” gereklidir.

Bilgi sistem denetçisi tarafından bu kontrollerin varlığının ayrıca etkinliğinin sorgulanması gerekir. Örneğin bilgi sistemlerinin yer aldığı bina ve odalarda yangın çıkması durumuna karşı bir önlem alınıp alınmadığı ve yangın çıkması durumunda bu sistemleri kurtarmak üzere belirlenmiş bir prosedürün var olup olmadığının tespit edilmesi gerekir (ÖEBSD Kılavuzu 2019: 9).

2.2.2.3.2. Sızma Testleri

Sızma, teknik olarak mümkün olan tüm yöntemlerin denenmesi ve hedef sistemlere saldırgan bir bakış açısıyla erişilerek sistemlere ulaşma işlemidir.

Sistemleri kapsamlı bir şekilde inceleyerek riskleri, güvenlik açıklarından kaynaklanan olası hasarları ve saldırganların ulaşabileceği yerleri analiz eder. Ayrıca Sızma testi, alanında uzman kişilerin bir kurumun altyapı, yazılım, donanım ve uygulamalar gibi bilgi sistemlerine bir saldırgan tarafından kullanılması beklenen araç ve teknikleri kullanarak sızması ve sonuçları raporlaması işlemidir. Sızma testi, zafiyet bulmanın yanı sıra zafiyetlerin değerlendirilmesini, sistemlere erişim yollarının bulunmasını ve yetkili erişimler elde edilmesini amaçlar. Ayrıca hedef sistemler üzerinde sisteme sızma, bilgilere erişme, etkiyi tanımlama gibi gerçekleştirilebilecek ek işlemlerin belirlenmesini sağlar. Sızma testinin genel amacı kurulu sistem veya uygulamadaki kör noktaları tespit etmek, potansiyel siber riskleri ortaya çıkarmak ve önerilen çözümlerle ilişkili riskleri yok etmek veya kapatmaktır.

BT altyapı sistemlerinin tamamı (SCADA, kablosuz ağ, VOIP sistemleri, kart sistemleri, sunucular, son kullanıcı bilgisayarları, güvenlik duvarı ürünleri vb.) sızma testlerine dâhil edilebilmekte ve siber risk ile ilgili sistemlerde kontroller yapılarak ayar yapılandırılmaları test edilebilmektedir (lostar.com.tr 21.08.2022).

Şekil 2.9: Sızma Testi Süreci (lostar.com.tr 21.08.2022)



Şekil 2.9' da sızma test süreci verilmektedir. Bu süreç aşamaları aşağıda açıklanmıştır.

Kapsam/Hedef Belirleme: Bir sızma testinin sızma/hedef aşamasının amacı, yapılacak sızma testinin hedeflerini ve testlerin gerçekleştirileceği sistemleri belirlemelidir. Müşteri ile yapılan görüşme sonrasında test edilecek sistemlerin tipine ve sayısına karar verilir. Test sırasında ortaya çıkan ancak kapsama dâhil olmayan varlıklar, müşteriyle görüşükten sonra teste dâhil edilebilir veya testten çıkarılabilir. Müşteri, test etmek istediği altyapı ve sistemler hakkında sızma testi yapacağı firmaya bilgi verir. Sızma testini yapan firma ise testlerde kullanılan IP adreslerini kuruma iletir. Böylece olası bir gerçek saldırı durumunda, bu olayların sızma testini yapan şirket tarafından değil, saldırgan tarafından gerçekleştirildiğini ortaya çıkarır (<https://statik.tse.org.tr> 18.08.2022)

Bilgi Toplama: Hedef ağ ve sistemler hakkında bilgilerin toplandığı aşamadır. İnternette halka açık kaynaklardan, OSINT (Open Source Intelligence) yöntemleri kullanılarak elde edilecek kişisel bilgiler, domain adresleri, IP adres aralıkları, cihaz listeleri vb. bilgiler alınır. Canlı sistemler, elde edilen bilgiler ve dâhili ağ testinde kullanılan IP aralıkları ile keşfedilir. Pasif (sistemde iz bırakmadan) çalışma öncelikle kapsamda belirtilen hedefler için yapılır. Saldırmanın bakış açısından pasif olarak sistem üzerinden ne kadar bilgi elde edilebileceği belirlenir. Bir sonraki adımda sızma testlerinin yapıldığı sistemin kullandığı altyapı, geliştiricinin hangi programlama dilini kullandığı, ilgili sistemlerin fonksiyonlarının neler olduğu, hangi işlemlerin ve testlerin yapılabileceği öğrenilerek bir sonraki güvenlik açığı tespitinde bu öğrenilen bilgiler kullanılarak testler yapılır (<https://statik.tse.org.tr> 18.08.2022).

Güvenlik Açığı Tespiti: Güvenlik açığı tespitinin ilk aşaması, otomatik araçlar kullanılarak sistemin genel olarak taranmasıdır. Bu otomatik araçlar sayesinde hangi servisin sistemin hangi portunda çalıştığı ve bu servisin hangi versiyonunun kullanıldığı gibi bilgilere ulaşılabilmektedir. Böylece, bu sürümdeki güvenlik açıkları doğrudan alınan sürüm bilgisinde tespit edilebilir (lostar.com.tr 21.08.2022).

Bilgi Analizi ve Planlama: Önceki adımda bulunan güvenlik açığının çözülmesi için gerekli araştırma ve planlama yapılır. Bir güvenlik açığından yararlanılırken yük olarak kullanılan exploit, payload vb. hazırlanır (<https://statik.tse.org.tr> 18.08.2022).

Saldırı ve Penetrasyon / Yetki Yükseltme: Hazırlanmış olan payload veya exploit güvenlik açığını sömürülmesi için hedef sistemde çalıştırılır. Çalıştırılan exploit'in sistemdeki işlevi ve diğer sistemlere etkisi incelenir. Daha sonra sistemde araştırma yapılarak diğer sistemlere sıçrama yapabilmesi araştırılır (<https://statik.tse.org.tr> 18.08.2022).

Zafiyet Taraması: Bir sistemde bir zafiyet bulunur ve yukarıdaki adımlar izlenir. Her bir zafiyet için tekrar tekrar bu adımlar gerçekleştirilir (lostar.com.tr 21.08.2022).

Sonuç Analizi-Raporlama: Önceki adımda uygulanan işlemlerin özeti çıkartılır. Oluşabilecek potansiyel zararlar, risklerin ortadan kalkması için alınabilecek önlemler, hangi sistemlerin etkilenebileceği ve bunun etkileri raporlanır (<https://statik.tse.org.tr> 18.08.2022).

Kılavuza göre Özel entegratörün aşağıdakiler kapsamında sızma testi yaptırması gerekir.

- “Ağ ve İletişim Altyapısı Testler
- İşletim Sistemi ve Platform Testleri
- Uygulama Testleri
- Veri Tabanı Testleri
- Web uygulamaları testler
- Mobil uygulama testleri”

Sızma testi; varlıklar ve bilgi sistemlerinin genelini kapsayacak biçimde, yılda en az bir kez olmak üzere tekrarlanır (ÖEBSD Kılavuzu 2019: 10).

Testlerde ortaya çıkan açıklara dair alınan önlemler, eylem planı şeklinde özel entegratör tarafından kayıt altına alınır. İlk denetim dışında, son iki sızma testi raporları ve alınan önlemlerinde bulunduğu kayıtlar denetim esnasında denetçiye ibraz edilir. Özel entegratör (ÖE), ilk denetim haricinde, ÖEBSD sırasında son iki sızma testi raporlarını ve alınan tedbirlerin yer aldığı kayıtları denetçiye ibraz eder. Bilgi sistemleri denetçisi sızma testlerinin uygunluğunu değerlendirecektir (ÖEBSD Kılavuzu 2019: 9).

2.2.2.3.3. Risk Yönetimi

Risk yönetimi, güvenliğin önemli olduğu bilgi sistemleri için temel bir gerekliliktir. Riski tanımlama, riski değerlendirme ve riski kabul edilebilir bir düzeye indirmek için

adımlar atma süreci olarak tanımlanabilir. Özel entegratör, bilgi sistemlerine ait tüm varlıkların risk analizini yapmalıdır. Her bir varlığın potansiyel riskleri, özelliklerine göre risklerin sınıflandırılması ve risklerden kaynaklanan hasar dereceleri “Risk Tablosu”nda belirlenmelidir. ISO 27001, ISO 22301 standartları kapsamında uygulanan risk işleme planı kabul edilebilir risk seviyesi, artık riskler, üst yönetime sunulur. Üst yönetim tarafından onaylanır (ÖEBSD Kılavuzu 2019: 10).

Risk yönetim planının onaylanmasının ardından operasyonel yöneticiler gerekli önlemlerin hayata geçirilmesi için çalışmalarını yürütürler. Her yıl veya önemli değişikliklerden sonra, bir önceki risk planının önlemlerinin uygulanması ve etkinliği değerlendirilerek yönetim gözden geçirme (YGG) üst yönetime sunulur. YGG raporları 10 yıl kadar özel entegratör tarafından saklanır. Bu raporların GİB tarafından istenilmesi halinde açıklanması zorunludur (ÖEBSD Kılavuzu 2019: 10).

Bilgi sistemleri denetçisi, işletmede bilgi sistemlerinin sağlamlığına ilişkin herhangi bir değerlendirme yapmadan önce mutlaka bu işletme tarafından benimsenen risk yönetimi politikalarını ve süreçlerinin incelenmesini yapmalıdır.

Bilgi Sistemleri Denetim ve Güvence Standartları 11 No’lu Standarda göre “*Bilgi sistemleri denetçisi, bilgi sistemleri denetim planının tamamını geliştirmede ve bilgi sistemleri denetim kaynaklarının etkili dağıtımı için önceliklerin belirlenmesinde kullanılacak uygun bir risk değerlendirme tekniği veya yaklaşımı kullanmalıdır. Bilgi sistemleri denetçisi, kişisel denetim planlamasında, denetlenen alanla ilgili riskleri tanımlamalı ve değerlendirmelidir*” (ISACA, 2010: 20).

2.2.2.3.4. İş Sürekliliği ve Felaket Kurtarma Merkezi (FKM) Yönetimi

İş Sürekliliği ve FKM Yönetiminin amacı, kuruluşun misyonunu hâla yerine getirebilmesini ve aşağıdakilere yol açan bir kesinti veya felaket durumunda muhafaza edilen bilgileri işleme, alma ve koruma yeteneğini kaybetmemesini sağlamaktır (ms.hmb.gov.tr 22.08.2022).

İyi tanımlanmış ve test edilmiş bir acil durum ve iş sürekliliği planının yokluğu veya yetersiz olması, bir felaket durumunda kuruluşun kendi varlığına yönelik aşağıdaki büyük tehditleri oluşturabilir:

- “Kuruluşun faaliyetlerini yeniden başlattıktan sonra misyonunu yerine getirememesi,
- Felakete maruz kalma olasılığının artması,
- Felaketin verdiği zararlarla başa çıkma imkânının azalması,
- Felaketten kaynaklanan kaybın veya zararın ağırlaşması,
- Yasal veya üçüncü kişilere karşı olan sorumlulukların zamanında yerine getirilememesi,
- Bir felaket durumunda iletişim imkânları, bilgi işleme kapasitesi, eğitilmiş insan kaynağı ve tüm varlıklar yitirilebileceğinden kurumun faaliyetlerini sürdürmesinde devamlılığın sağlanamaması” (Sayıştay, 2013: 99).

Özel entegratör, sunduğu hizmetin kesintisiz devamını sağlayabilmek için İş Sürekliliği ve Acil Durum Prosedürünü hazırlar, kullanır. Bu prosedür, risk yönetimi ilkeleri ve risk değerlendirme tablosu ile bağlantılı olmalıdır. Planlı bakıma ek olarak, bilgi sistemleri her ay %99,75 kullanılabilirlikle hizmet verecek bir altyapıda olmalıdır. (ÖEBSK Kılavuzu 2019: 10).

Hazırlanan prosedürler dikkate alınarak bilgi sistemlerinin ayakta kalma süreleri takip edilir, kaydedilir. Sistem performansı 2 ay üst üste gelecek şekilde ya da yılda en az 3 defa hedefin altında kalması halinde, iyileştirme planı hazırlanır, en geç 3 ayda faaliyete geçirilir. Yapılan tüm bu işlemler kayıt altına alınır, 10 yıl muhafaza edilir. Bilgi sistemlerinde veri tabanı, uygulama sunucuları, aktif ağ cihazları, güvenlik duvarları gibi kritik önemdeki altyapılar aktif yedekli çalıştırılır (ÖEBSK Kılavuzu 2019: 10).

İş sürekliliğinin sağlanması için, önceden planlanmış senaryolara göre risklerin gerçekleştiğinin varsayıldığı tatbikatlar yapılır. Her yıl bir defa en az iki ayrı senaryoda hazırlanan tatbikat yapılır, kayıt altına alınır. Hizmet kesintisi ivedilikle tespit edilebilmeli bunun için acil uyarı sistemleri kurulmalıdır (ÖEBSK Kılavuzu 2019: 10).

İş sürekliliğinin diğer bir parçası felaket kurtarma merkezidir (FKM).Ö.E, aşağıdaki işlevleri sağlayan bir felaket kurtarma merkezini işletmek zorundadır. FKM coğrafi olarak özel entegratörün konumundan farklı bir ilde bulunmalıdır. Entegratör veri tabanının en çok 30 dakika gecikme ile alınan yedeği FKM de olmalıdır. Böylesi bir öneme sahip olan FKM, diğer sistem odalarındakine benzer aynı nitelikte olan fiziksel, elektronik koruma önlemleriyle donatılmalıdır. Ana sistemlerde bir kesinti yaşanması durumunda özel entegratör hizmeti FKM üzerine alabilecek şekilde FKM’yi

yapılandırmış olmalıdır. Bu hizmetin verilmesi, kesinti yaşandıktan hemen sonra 6 saati aşmamalı ayrıca ISO 223012'e uyan bir altyapıda olmalıdır (ÖEBSD Kılavuzu 2019: 10).

Bilgi sistem denetçisi ise, işletmenin İş Sürekliliği ve FKM Yönetiminin varlığını, acil ve beklenmedik durumlara ilişkin işletmenin risk analizlerini inceleyerek bu kontrollere ilişkin değerlendirmelerini yapmış olacaktır.

2.2.2.3.5. Değişiklik Yönetimi

Sistemlerin yapması gerekeni yapmaya devam ettiğine ve kontrollerin amaçlandığı gibi çalışmaya devam ettiğine dair güvence elde etmek için değişiklik kontrollerine ihtiyaç vardır (IT Audit Manual 2017: 18).

Değişiklik hem donanım hem de yazılımdaki değişiklikleri ifade eder. Donanım, bilgisayarları, çevre birimlerini ve ağları içerir. Yazılım, hem sistem yazılımını (işletim sistemi ve yardımcı programlar) hem de bireysel uygulamaları içerir.

Aşağıdaki nedenlerle değişiklik talep edilebilir:

İşlevsellik Geliştirme: Günlük sistem kullanıcıları, sistemin işlevselliğinden memnun olmayabilir. Bu durum örneğin sahip oldukları ekranlardan, sistem yanıt süresinden hoşnutsuzluk olarak görülebilir (IT Audit Manual 2017: 18).

Kapasite Planlama: Sistem ek kaynaklar veya artırılmış kapasite bileşenleri gerektirebilir.

Güvenliği Artırmak için: Bilgi teknolojileri güvenlik personeli sistem güvenliğindeki tespit edilen zayıflıklar, güvenliği iyileştirmesi gereken değişiklik taleplerine neden olabilir (IT Audit Manual 2017: 18).

Rutin Güncellemeler: Sistem geliştiricileri sistem yazılımını güncelleyebilir ve iyileştirebilir.

Gereksinimlerdeki Değişiklikler: Mevzuattaki, iş gereksinimlerindeki veya iş yönündeki değişiklikler, finansal sistemin değiştirilmesini gerektirebilir.

Yetersiz değişiklik kontrolleriyle ilişkili riskler aşağıdaki gibidir:

Yetkisiz Değişiklikler: Sistemlerde kazara veya bilinçli olarak yapılmış ancak yetkisiz değişikliklerdir. Örneğin, yetersiz kontroller varsa, uygulama programcıları canlı ortamdaki programlarda yetkisiz değişiklikler yapabilir;

Uygulama Sorunları: İş gereksinimleri için değişikliğin zamanında olmadığı durumlarda ortaya çıkan sorunlardır (Örn. yıllık vergi oranları).

Hatalı İşleme ve Raporlama: Amaçlandığı gibi işlemeyen sistemlerdir. Bu, hatalı ödemelere, yanıltıcı raporlara, yanlış işlemlere ve nihai olarak nitelikli hesaplara yol açabilir.

Yetkisiz Donanım ve Yazılım Kullanımı: kullanımda olan ve yetkilendirilmemiş sistemler (Donanım ve Yazılım): Bu, sistemin farklı bölümleri arasında uyumsuzluğa veya telif hakkı mevzuatının ihlaline neden olabilir (IT Audit Manual 2017: 18).

Sistem konfigürasyonlarındaki tüm değişikliklerin yetkilendirildiğinden, test edildiğinden, belgelendiğinden, kontrol edildiğinden ve sistemlerin amaçlandığı gibi çalıştığından emin olmak için değişiklik kontrolleri uygulanır.

Özel entegratör, hizmetlerini gerçekleştirmek için kullandığı yazılımların değişiklik yönetimini yapar. Bu yazılımlar için geliştirme ortamı, yazılımın ve bileşenlerinin önceki tüm sürümlerinin yönetimine izin verecek şekilde yapılandırılmalıdır. Yazılım ve bileşenlerinin geçmiş sürümleri ve yapılan değişiklikler, değişikliğin amacı, ne zaman, kim tarafından yapıldığına dair bilgilerin bulunması şartıyla erişilebilir olmalı ve 5 yıl boyunca saklanmalıdır. Yazılım geliştirme, test ortamı ve canlı ortam aynı alt ağda olmamalıdır. Testin yapıldığı ortamda kullanılan verilerin güvenlik için canlı ortamdaki farklılaştırılması gerekir. Test edilen yazılım veya bileşenlerin dağıtımı, yetkili personel tarafından canlı ortama aktarılmalıdır (ÖEBSK Kılavuzu 2019: 11).

Bilgi sistemleri denetçisi tarafından işletmenin bilgi sistemlerine yönelik değişikliklerine veya yeni sistem geliştirme projelerine yönelik politikalarının, hazırlanan projeyi yönetecek ekibin yeterli nitelik ve deneyime sahip olup olmadığı, projenin işletme hedeflerine uygun olup olmadığı, projenin gerçekleştirilebilirliğine yönelik önceden hazırlanmış teknik, mali ve sosyal analizlerin yapıp yapılmadığının sorgulanması gerekir. Söz konusu sorgulamalar denetçinin bu kontrole yönelik olarak değerlendirmesini yaparken yardımcı olacaktır.

2.2.2.3.6. Denetim İzlerinin Oluşturulması ve Saklanması

ÖE, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef, GİB iletiliminde kullanılan yazılım uygulamaları, veri tabanı motorları, uygulama kayıtlarını muhafaza eder.

“Bu kayıtlarda, işleme ilişkin ağ trafiği bilgisine ek olarak asgari aşağıdaki bilgiler bulunur:

- *İşlemi gerçekleştiren uygulama,*
- *İşlemi gerçekleştiren ve varsa onaylayan yetkili kişiler veya yetkisiz erişim kayıtları,*
- *İşlemin açıklaması,*
- *Yapılan işlemin zaman bilgisi,*
- *İşlemin olumlu veya olumsuz olmak üzere sonucu,*
- *Etkilenen veri ve sistemlerin bilgisi.”*

ÖE denetim izi kayıtları bütünlüğünü koruyabilmek için tedbir almalıdır. Bu tedbirler için, bir defa yazma, birden fazla kez okuma özelliği olan cihazlar kullanılabilceği gibi, zaman damgası da kullanılabilir. Kayıtlar en az 10 yıl süre ile muhafaza edilir, istenildiği takdirde GİB yetkilileri ya da denetçiler tarafından ulaşılabilmesi için erişimine açılır (ÖEBSK Kılavuzu 2019: 11).

Denetim izi kayıtlarını tutan sistemlerin arızalanması durumunda acil ve otomatik uyarı mekanizmaları kurulmuş olmalıdır. Bu sistemlerin işleyişi ilgi personelce ayda bir defa gözden geçirilip 3 ayda bir defa yapılacak toplantılarda değerlendirilir (ÖEBSK Kılavuzu 2019: 11).

Bilgi sistemleri denetçisi özel entegraötürün “denetim izleri yönetimi” kurallarına uygululuğunu kontrol edecektir.

2.2.2.3.7. Dış Hizmet Alımı

ÖE, bilgi sistemlerinin temini, işletimi ya da bakımı için dış hizmet alımından faydalanabilir. Dış hizmet alınması durumunda taraflar arasında alınan hizmetin türü, konusu, kapsamı, işin süresi, tarafların açık unvan ve adresleri ile hak ve

sorumluluklarının yer aldığı bir sözleşme yapılır. Entegratör bu sözleşmeyi istenildiği takdirde ibraz etmek üzere, 10 yıl kadar saklar (ÖEBSK Kılavuzu 2019: 12).

Sözleşme yürürlüğe girdiği andan itibaren en fazla 15 günde özel entegratörün GİB'e bildirim yapması gerekmektedir. Aynı şekilde, süresi sona eren ya da süresinden önce bitirilen sözleşmeler de en fazla 15 günde GİB'e bildirilir (ÖEBSK Kılavuzu 2019: 12).

“Özel entegratör, dış hizmet alımı yaptığı tedarikçide kriptografik anahtarlar için kullanılan özel donanım güvenlik modülleri (HSM) de bulunduruyorsa, bu cihazların münhasıran kendisine adanmış olması şartının da sözleşmede yer alması gerekir.”

Kılavuzda tanımlanan özel entegratörün yükümlülükleri, dış kaynak kullanımı nedeniyle değişmeden kalır. Tüm yükümlülükler taşeronunda da aranır (ÖEBSK Kılavuzu 2019: 12).

Bilgi sistemleri denetim faaliyetleri dış hizmet alımının yapıldığı taşeronunda gerçekleştirilir. Bu sorumluluk yapılan sözleşmede açıkça belirtilmelidir. *“Denetçinin dış hizmet alımı yapılan taşeronun, alıma konu olan tesis, teçhizat ve mekanlarına erişiminin engellenmesi, denetim görüşünün “olumsuz” olması için yeterlidir.”* (ÖEBSK Kılavuzu 2019: 13).

2.2.2.3.8. Personelin Niteliğine İlişkin Gereksinimler

ÖE verilen hizmete uygun sayıda ve kalitede personel istihdam etmekle veya dış hizmet yoluyla iş gücü sağlamakla yükümlüdür. Bu yükümlülük gereği *“ağ ve ağ güvenliği uzmanı, veri tabanı uzmanı, sistem uzmanı, kalite sistemleri uzmanı, yazılım geliştirme uzmanı, konfigürasyon yöneticisi ve test uzmanı rollerinde personel istihdamı zorunludur”*. Bu görevlerde ikiz rol kabul edilemez. Dış hizmet alımı yapılması durumunda, belirtilen personellerin bir kısmının sözleşmeye göre dış hizmet sağlayıcısı tarafından temin edilmesi yeterli olabilir. Bu durum hakkındaki son karar bilgi sistemleri denetçisine aittir (ÖEBSK Kılavuzu 2019: 12).

Bilgi sistemlerinin yönetilmesinde, işletilmesinde, veri tabanının, uygulamaların geliştirilmesinde, teste tabi tutulmasında, görev ve sorumlulukların ayrılığı kuralı dikkate alınır. Bu kural gereği, bu roller farklı kişilerce yerine getirilir. Aynı kişi birden fazla görev yapamaz. Bu sistemlerin tasarımı bu kuralın uygulanmasına imkân sağlayacak

şekilde yapılır. Çalışan personelin eğitimi, sertifikasyonları gerçekleştirdiği görev ile uygun olmalıdır.

Özel entegratör, yönetim kurulu kararı ile belirlediği organizasyon şemasını, çalışan personele ait bilgileri 15 gün içerisinde GİB e iletir. Aynı şekilde işten ayrılan personel hakkında da GİB e bilgi iletilir (ÖEBSD Kılavuzu 2019: 12).

Bilgi sistemleri denetçisi personelin niteliğine ilişkin kontrol tablosunda yer alan maddelere göre değerlendirme yapacaktır.

2.2.2.3.9. Uluslararası Standartlara İlişkin Sertifikasyonlar

GİB tarafından hazırlanan kılavuzda “*Özel entegratör, bilgi sistemlerinin tamamını içerecek bir kapsamdan daha dar olmamak üzere, aşağıdaki sertifikasyon belgelerine sahip olmalıdır:*

ISO/IEC 20000:1 2011 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi

ISO/IEC 27001:2013 Bilgi Güvenliği Yönetim Sistemi Belgesi

ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi” (ÖEBSD Kılavuzu 2019: 13).

2.2.2.3.10. ÖEBSD Değerlendirme Sınıfları

Bilgi sistemleri denetçisi kılavuzda belirtilen aşağıda yer alan 12 kontrol grubu ile ilgili hazırlanan tablolarda yer alan toplam 208 kontrol maddesine göre denetim görüşü oluşturacaktır. Aşağıda bu kontrol gruplarını değerlendirme sınıfları hakkında kısaca bilgi verilmiştir (ÖEBSD Kılavuzu 2019: 15).

2.2.2.3.10.1. Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu (ÖEBSD_SER)

Bu değerlendirme sınıfı, özel entegratörlerin sağlaması gereken uluslararası sertifikasyonların varlığı ve uygunluğu ile sızma testlerinin uygunluğunun bilgi sistem denetçisi tarafından kontrol edilmesini amaçlamaktadır. Bu sınıf altında iki alt bileşen tanımlanmıştır:

“ÖEBSD_SER.1: *Bu değerlendirme alt bileşeninde denetçiden özel entegratörün aşağıda uluslararası sertifikasyonları sahip olduğunu teyit etmesi istenmektedir:*

- *ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi*
- *ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi*
- *ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi*
- *Son yapılan sızma testi raporu*
- *Güncel BİS Raporu*

ÖEBSD_SER.2: *Bu değerlendirme alt bileşeninde denetçiden, özel entegratörün iç kontrol ve denetim süreçlerinin varlığını ve çıktılarının uygunluğunu kontrol etmesi beklenmektedir” (ÖEBSD Kılavuzu 2019: 15).*

2.2.2.3.10.2. Personelin Niteliği (ÖEBSD_PER)

“Bu değerlendirme sınıfında, özel entegratörün, verdiği özel entegratörlük hizmetine uygun nitelikte ve sayıda personel istihdam edip etmediği kontrol edilecektir” (ÖEBSD Kılavuzu 2019: 15).

2.2.2.3.10.3. Sistem ve Güvenlik Değerlendirme Sınıfı (ÖEBSD_SIS)

“Bu değerlendirme sınıfı, özel entegratörlerin bilgi sistemlerinde uyması gereken alt yapının, sistem mimarisi ve benzeri her türlü fiziki unsur ile iş sürekliliğinin temininin, gerekli güvenlik ve risk değerlendirme süreçlerinin oluşturulmasının, işletilmesinin, değişiklik yönetiminin, denetim izlerinin oluşturulmasının ve dışarıdan hizmet alınması durumundaki gerekliliklerin kontrol edilmesini amaçlamaktadır.

Bu değerlendirme sınıfının olduğu 7 alt bileşen aşağıda açıklanmıştır” (ÖEBSD Kılavuzu 2019: 15).

“ÖEBSD_SIS.1 Fiziki Şartlar ve Güvenlik Tedbirleri: *Özel entegratörün sağlaması gereken uluslararası sertifikasyonları varlığı ve uygunluğu ile sızma testlerinin uygunluğu kontrol edilecektir.*

ÖEBSD_SIS.2 Erişim Güvenliği: *Özel entegratörün bilgi sistemlerinin sağlaması gereken fiziki ve elektronik erişim güvenliği kontrol edilecektir.*

ÖEBSD_SIS.3 İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları: Özel entegratörün “İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları” kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.4 Değişiklik Yönetimi: Özel entegratörün “Değişiklik Yönetimi” kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.5 Denetim İzleri Yönetimi: Özel entegratörün “Denetim İzleri Yönetimi” kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.6 Dış Hizmet Sağlayıcılarının Yönetimi: Özel entegratörün “Dış Hizmet Sağlayıcılarının Yönetiminin” kurallara uygunluğu kontrol edilecektir.

ÖEBSD_SIS.7 Hizmet Yazılımlarına İlişkin Kontroller: Özel entegratörün hizmetlerinde kullandığı uygulama yazılımlarının, ilgili GİB kılavuzları, e-Fatura, e-Saklama, e-Arşiv, e-İrsaliye, e-Defter ve e-imza standartları ve hizmetin akışına uygun normları taşıyıp taşımadığı kontrol edilecektir.”

Değerlendirme alt bileşenlerine ilişkin kontrol tabloları eklerde verilmiştir.

2.2.2.3.11. Raporlama

Bilgi sistemleri denetçisinin görevi, bilgi sistem süreçleri üzerindeki kontrollere dair denetim kanıtları toplayıp, değerlendirmek ve elde edilen kanıtlara dayanarak denetim görüşü oluşturmaktır. Denetçi, denetimi, denetim görüşünde yeterli güvence sağlayan gerçeklere ve kanıtlara dayanarak gerçekleştirir.

ÖEBSD raporu, önemlilik kavramını dikkate alınarak, bilgi sistemleri denetçisinin özel entegratörün sistemlerini değerlendirdiği, oluşan düşüncesinin açık bir ifade ile yazılı bir biçimde sunulduğu metindir. Bu amaçla, bilgi toplamak, gözlem yapmak, sorgulamak, yeniden gerçekleştirmek veya hesaplamak ve analitik akıl yürütmek denetim faaliyetinin esasını oluşturur. Bilgi sistemleri denetçisi denetimi GİB tarafından hazırlanan kılavuzu esas alarak gerçekleştirir. Kılavuzda yer almayan veya yorumu belirsiz bir sorun ortaya çıkarsa, uluslararası geçerliliği olan bilgi teknolojisi kontrol hedeflerini sunan ISO standartları ya da COBIT belgelerinde belirlenen prosedür ve ilkeleri dikkate alınır. Böyle bir durumda faydalanılan kontrol, gerekçesi ve değerlendirmesiyle denetim raporunda ek olarak açıklanır.

“ÖEBSR Raporu, “Denetim görüş yazısı” ve “Rapordan” oluşur. “Denetim görüş yazısında”, denetimin yeri, tarihi, denetlenen özel entegratörün unvanı, denetçi veya denetçilerin isimleri ve unvanları ile denetim görüşü, “olumlu”, “şartlı”, “olumsuz” veya “görüşten kaçınma” şeklinde yer alır.” (ÖEBSR Kılavuzu 2019: 14).

“Denetçi, EK 1’de verilen 12 kontrol tablosunda yer alan toplam 208 kontrol maddesine göre denetim görüşünü oluşturacaktır. Görüşün oluşturulmasında, denetçinin uygulayacağı ilkeler kılavuzda aşağıdaki gibi açıklanmıştır. Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamıyorsa (G) harfini yazacaktır (ÖEBSR Kılavuzu 2019: 14).

- “Olumlu görüş” için, 208 kontrol maddesinin en az 166 maddesinin yanıtı “E” olmalı,
- Maddede belirtilen koşul sağlanmış olsa dahi, herhangi bir değerlendirme sınıfından “E” yanıtlarının sayısı %70’in altında kalıyorsa “olumlu görüş” verilemez. %70 için hesaplanacak madde sayısı, o değerlendirme sınıfındaki toplam kontrol maddesinin %70’i tam sayıya karşılık gelmiyorsa, bulunan sayıdan küçük en büyük tamsayıdır.
- “Olumlu görüş” verilememiş ise, verilecek görüş; “H”, “K” veya “G” cevaplarından sayısı fazla olana göre, sırasıyla “olumsuz”, “şartlı görüş” veya “görüşten kaçınma” kanaatine varılır.”

Denetçi, kanaatinin oluşmasına dayanak bulgularını raporunda açıkça yazar. Ortaya çıkarılan eksikliklerin, varsa kısa bir zaman içinde ya da daha sonraki denetim gerçekleşene kadar tamamlanması gereği hakkındaki görüşler ile denetim görüşüne temel oluşturacak tespitler raporda belirtilir. Bununla birlikte denetçi, bu kılavuzda açıkça yazılmamış olsa dahi, her türlü görüş ve önerisine denetimin amacı ve kapsamına uygun olmak kaydıyla raporunda ayrıca yer verebilir (ÖEBSR Kılavuzu 2019: 33).

2.2.2.3.12. ÖEBSR Raporuna Bağlı Olarak GİB Tarafından Uygulanacak Yaptırımlar

“GİB, ÖEBSR raporunun sonuçlarına göre farklı yaptırımlar uygulayabilir. Buna göre rapor sonucunun olumlu olması halinde özel entegratör, varsa kendisine tebliğ

edilen eksikliklerin veya iyileştirmelere ilişkin alacağı tedbirleri içeren eylem planını ve buna ilişkin faaliyetleri ve tamamlama sürelerini GİB'e 15 gün içinde bildirir. Buna uymayan özel entegratör bir yazıyla uyarılır. GİB, eylem planına ilişkin tamamlama sürelerinde değişiklik yapmaya yetkilidir” (ÖEBSK Kılavuzu 2019: 14).

“Şartlı görüş veya görüşten kaçınma halinde, özel entegratör ivedilikle bir yazıyla uyarılır ve denetimi en geç 90 gün içinde tekrarlaması istenir. Üst üste 2 kez şartlı görüş veya görüşten kaçınma olması durumunda, özel entegratörün faaliyeti, olumlu görüş alacağı yeni bir denetim sonucuna kadar askıya alınır. Faaliyetin askıya alınması nedeninin 2 kez üst üste görüşten kaçınma olması durumunda, faaliyetin askıya alınma süresi 3 aydan daha kısa olamaz” (ÖEBSK Kılavuzu 2019: 14).

“Rapor sonucunun olumsuz olması halinde özel entegratörün faaliyeti ivedilikle geçici süreyle durdurulur. 6 ay içinde olumlu görüş bildiren yeni bir denetim raporunun GİB'e ibraz edilmemesi halinde özel entegratörün yetkisi iptal edilir. Özel entegratör, 6 ay içinde yapacağı her yeni denetime ilişkin, denetim öncesinde ve sonrasında GİB'i bilgilendirmekle mükelleftir” (ÖEBSK Kılavuzu 2019: 14).

2.2.3. E-Belge Özel Entegratörleri Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi

Finansal bilgiler, işletmenin mevcut sistemleri üzerinde ve bu sistemlerde yer alan raporlar temel alınarak hazırlanır. Finansal denetimin üzerinde çalıştığı bu veriler günümüzde bilgi sistemleri tarafından üretilir. Bu sebeple bilgi sistemlerinin sözü edilen verileri doğru üretilip üretilmediği finansal denetimin doğruluğunu, anlamlılığını doğrudan etkiler.

Değişen teknoloji ve elektronikleşen kayıt ortamı, bilgi sistemlerinin de denetlenmesi ihtiyacını doğurmuştur. İşletmelerde bilgi sistemlerinin kullanımı denetim kanıtını, takibini, iç kontrol yapısını etkilemekte, yeni hile, hata mekanizmalarını ve fırsatlarının ortaya çıkmasına neden olmaktadır. Bağımsız denetçi, denetim sürecini etkileyebilecek bu yeni riskleri dikkate almalıdır. Denetçi, bilgi sistemleri alanına uyum sağlamalı ve elektronik bilgi ortamının denetim süreci üzerindeki etkisini doğru bir şekilde değerlendirmelidir (Özbilgin, 2012: 164).

Sermaye Piyasası Kurulu bilgi sistemleri bağımsız denetim tebliğinin, bilgi sistemleri bağımsız denetimi ile bağımsız denetimin ilişkisi Madde 9 da;

“MADDE 9 – (1) Bağımsız denetim ile bilgi sistemleri bağımsız denetimi, birbirlerinin kapsam ve sonucunu etkileyecek hususlar ihtiva etmeleri nedeni ile etkileşimli bir yaklaşım içinde planlanır ve uygulanır.

“(2) Bilgi sistemleri denetçisi, bilgi sistemleri bağımsız denetiminin kapsamını belirlerken ve bu kapsamdaki çalışmalarını yürütürken; denetim görüşünü destekleyecek düzeyde yeterli denetim kanıtı elde edilmesinin yanı sıra, bağımsız denetime ilişkin denetim riski değerlendirmelerini desteklemek için de denetim kanıtı elde edilmesini gözetir.

“(3) Bilgi sistemleri bağımsız denetimine ilişkin görüşün “şartlı”, “olumsuz” ya da “görüş bildirmekten kaçınma” şeklinde olması durumunda; görüş ve görüşe esas teşkil eden tespitler bağımsız denetçiye yazılı olarak iletilir. Bu husustaki sorumluluk Kurum, Kuruluş ve Ortaklıkların yönetim kuruluna aittir.

(4) Bağımsız denetçi tarafından, bağımsız denetim çalışmalarında kullanılmak üzere bilgi sistemleri ve denetimine ilişkin talep edilen bilgi ve belgelerin, bilgi sistemleri denetçisi tarafından bağımsız denetçiye iletilmesi esastır.” açıklanmıştır.

e-dönüşüm kapsamında yer alan, bağımsız denetime kanıt niteliği taşıyan e-fatura, e-defter, e-arşiv vb. uygulamaları aracılık hizmeti ile yerine getiren e belge özel entegratör kuruluşların bilgi sistemleri denetiminin bağımsız denetimi etkilediği düşünülmektedir.

“ÖEBSD’ de, sistemler açısından veri giriş kontrolleri, veri işleme kontrolleri ve yetki kontrolleri detaylı olarak incelenir. Kaynak verilerin sağlıklı bir şekilde sisteme girilme durumu, sistem içinde işlenirken herhangi bir bozulmaya uğrayıp uğramadığı, söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenir.”

Bu kapsamda hazırlanacak raporların doğruluğunu sağlamak için hazırlanan çapraz kontroller gözden geçirilir. Daha sonra sistemler ve raporlar ile mali tablolar arasındaki geçişi varlık, tamlık ve doğruluk açısından ele alınır. Varlık, tamlık ve doğruluk ölçüleri, finansal tabloları oluşturan veri olgularıdır. Yapılan işlemler raporlarda yer alan bilgilerin bozulmadan tam olarak mali tablolara yansıtılıp yansıtılmadığını belirler.

e-Belge özel entegratör bilgi sistemleri denetiminin bağımsız denetime etkisi risk değerlendirmesi, iç kontrol ve denetim kanıtları konuları dikkate alınarak incelenmiştir.

“Bağımsız denetçi denetim planlaması aşamasında denetim alanı ile ilgili riskleri değerlendirmektedir. Bu aşamada denetçi, bilgisayarlı bilgi sistemi çevresi ve bu çevrenin doğal risk ve kontrol riski değerlendirmesini etkileyip etkilemediği konusunda bir anlayış oluşturmalıdır” (ISA 401: 7). Elektronik bilgi sistemlerinde hata veya hile sonucu ortaya çıkan yanlış uygulamalar iç kontrol sistemlerinin etkili şekilde çalışmasını engellemektedir. Denetçinin bilgi sistemlerinde bulunan önemli yanlışlıkları ortaya çıkarmaması durumunda yüksek değerlendirilmesi gereken kontrol riski düşük değerlendirilebilir. Bilgi sistemleri, denetçinin iç kontrollere duyduğu güveni hatalı şekilde artırabilir ve denetim çalışmasının kapsamı yanlış görüş sunulmasına yol açacak şekilde daraltılabilir. Bilgi sistemlerinde önemli bir yanlışlık olmadığı halde denetçinin sistemde önemli bir yanlışlık olduğu kanaatine varması ve iç kontrol sistemine güvenmemesi durumunda ise kontrol riski hatalı şekilde yüksek değerlendirilebilir ve denetim çalışmasının kapsamı gereksiz şekilde genişletilerek zaman kaybına sebep olunabilir. Bu nedenle bağımsız denetim çalışmasında bilgi sistemleri, iç kontrol sisteminin bir parçası olarak denetlenmeli ve elde edilen sonuçlar kontrol riski değerlendirmesinde dikkate alınmalıdır. Denetçi doğal riskin ve kontrol riskinin düşük olduğu durumlarda tespit riskini yüksek değerlendirmekte ve daha az denetim kanıtı elde ederek finansal tabloların doğru şekilde sunulduğu konusunda güvence sağlamaktadır. Ters durumda ise denetçinin finansal tabloların doğru şekilde sunulduğu konusunda ikna olması için daha çok denetim kanıtına ihtiyaç duyulmaktadır. Bu nedenle e belge özel entegratörleri bilgi sistemleri denetim sonuçları bağımsız denetimi etkiler. ÖEBSD denetçinin risklerin tespiti ve yönetilmesine ilişkin sorumluluğunu yerine getirmesine katkı sağlar (Özarlan, 2014: 156)

Bağımsız denetçi denetim sürecinde zaman ve kaynak tasarrufu sağlamak amacıyla iç kontrollerden güvence elde edebilmeyi amaçlamaktadır. “İç kontrol hakkında güvence elde etmek ise denetlenen kurumu tüm yönleriyle tanımaya, kurumun içinde bulunduğu kontrol ortamını, muhasebe, bilgi sistemlerini anlayıp değerlendirmek suretiyle kuruma ilişkin riskleri tanımlayabilmeye ve denetimini bu riskleri baz alarak tasarlamaya bağlı olmaktadır” (Sayıştay, 2011: 16). Bu kapsamda finansal denetimin amacına uygun olarak ÖEBSD nin yürütülmesi finansal denetim aracılığıyla tespit edilemeyen kontrol zayıflıklarının tespit edilebilmesini sağlamaktadır. Ayrıca e-belge

özel entegratör bilgi sistem denetimi denetçinin finansal tablo denetiminde iç kontrol sistemini dikkate alma sorumluluğunu yerine getirmesine katkı sağlar.

Denetçinin, görüşüne dayanak oluşturan sonuçlara ulaşırken kullandığı bilgilere denetim kanıtı denir. Denetim kanıtları, finansal tablolara dayanak (temel) oluşturan muhasebe kayıtlarındaki bilgiler ile diğer kaynaklardan elde edilen bilgileri içerir. Bağımsız denetimi gerçekleştiren denetçi işletmenin finansal raporları hakkında görüşünü kaliteli ve nitelikli kanıtlara dayandırmalıdır. Muhasebe sistemlerinde bilgisayarların kullanılmaya başlanması denetim kanıtlarının yapısını da etkilemekte ve değiştirmektedir. Denetim kanıtları basılı çıktı olarak bulunmamakta, bilgisayar ortamında tutulmaktadır. Denetçi, bilgi sistemlerinin etkin ve etkili şekilde çalıştığı konusunda görüş oluştururken, görüşünü elektronik kanıtlara dayandırmaktadır. Denetçi, denetim kanıtının denetim görüşünün oluşturulmasında yeterli ve güvenilir nitelikte olup olmadığını değerlendirmelidir. Denetçi güvenilirliğe ilişkin değerlendirmelerinde elektronik denetim kanıtına özgü şartları dikkate almalıdır. Elektronik bilgilerin güvenilirliği, elektronik bilgi sistemleri ile elektronik bilgi sistemlerini destekleyen teknolojilerin güvenilirliğini sağlamakla elde edilebilir (Şirin 2012, 54). Elektronik ortamlarda kanıt toplarken geleneksel denetim yöntemlerinde olduğu gibi basılı belgelere odaklanmak yerine elektronik sistemlerin çalışmasını değerlendirmek ve elektronik ortamlarda kanıtın güvenilirliğini sağlamak denetçinin değerlendirmesi gereken bir konudur. Elektronik denetim kanıtları basılı belgelere oranla daha kolay silinebilir, değiştirilebilir, yolsuzlaştırılabilir veya çoğaltılabilir niteliktedir. Elektronik ortamlarda sistem güvenilirliği ancak etkin ve etkili şekilde gerçekleştirilen bilgi sistemi denetimi çalışması ile sağlanabilir. e-fatura, e-defter v.b elektronik belgelerde bağımsız denetçinin görüşüne etki edecek kanıtlardır. Bu nedenle bu kanıtların oluşturulduğu e belge özel entegratörleri bilgi sistemlerinin denetimi bağımsız denetimi etkiler. Bu sistemlerdeki bir yanlışlığın ortaya çıkarılamaması, hatalı bir kanıtın güvenilir kanıt biçiminde denetçinin karşısına çıkmasına yol açabilir. Denetim görüşü, gerçekte hatalı olan fakat güvenilir kanıt niteliği taşıyan kanıtlara dayandırılabilir. Bu kanıtlar yanlış denetim görüşünü desteklemekte kullanılmış olur. Kanıtın yapısını değiştiren bilgi sistemlerinin göz ardı edilerek yalnızca çıktılara odaklanması, bağımsız denetimin hatalı kanıtlar üzerinden gerçekleştirilmesine bağlı olarak yanlış denetim görüşünün sunulmasına sebep olur.

Bilgi sistemleri siber saldırıları, son kullanıcı hataları, donanım ve yazılım hataları, doğal afetlerden kaynaklı sorunlar, enerji problemleri, veri ve programlara yetkisiz erişimin, bağımsız denetim üzerinde olumsuz etkisi vardır. Ayrıca altyapı yetersizlikleri ve performans sorunu bağımsız denetimi etkiler.

Sonuç olarak, günümüzde bilgi çağında ve küreselleşmenin getirdiği rekabet ortamında bilgi sistemleri işletmelerin faaliyetlerinin ayrılmaz bir parçası olduysa aynı şekilde ihtiyaca paralel olarak bilgi sistemleri denetimi de finansal denetimin ayrılmaz bir parçası haline dönüşmüştür. Bağımsız denetçi bilgi sistemlerinin içyapısında bulunan önemli bulunan hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır.

Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır. Bilgi sistem denetimi bağımsız denetimin güvenilirliğine katkı sağlar.

ÜÇÜNCÜ BÖLÜM

3. BAĞIMSIZ DENETÇİLERİN BİLGİ SİSTEMLERİ DENETİMİNİN BAĞIMSIZ DENETİME ETKİSİ KONUSUNDAKİ GÖRÜŞLERİ VE E-BELGE ÖZEL ENTEGRATÖRLERİ BİLGİ SİSTEM DENETİMİNE İLİŞKİN BİLGİ DÜZEYLERİNİN ARAŞTIRILMASI: ANKARA İLİ UYGULAMASI

Bu bölümde bilgi sistemleri denetiminin bağımsız denetime etkisini ölçmek amacıyla bağımsız denetçiler üzerine bir araştırma yapılmıştır. Bu amaçla Ankara ilinde faaliyet gösteren bağımsız denetim kuruluşlarında çalışan bağımsız denetçiler ile anket uygulaması yapılmış olup elde edilen veriler analiz edilmiştir. Ayrıca bu bölümde araştırmanın konusu, amacı ve önemi, veri toplama yöntemi ile araştırmanın teorik modeli ve hipotezler yer almaktadır.

3.1. Araştırmanın Konusu, Amacı ve Önemi

Günümüzde işletmeler artan rekabet ortamında etkisiyle daha detaylı, kaliteli ve hızlı bilgiye ihtiyaç duymaktadır. Bu ihtiyacın artması günümüzdeki bilgi artışı ile bir araya geldiğinde, hemen hemen tüm kuruluşların muhasebe fonksiyonu da dahil olmak üzere iş süreçlerini bilgi sistemlerinin desteği ile yönetmelerini zorunlu kılmıştır. Özellikle teknoloji odaklı ve finansal işlem miktarı yoğun işletmelerde, muhasebe ve finansal raporlama süreçlerinin bilgi sistemlerine dayandığı görülebilmektedir. Muhasebe ve finansal raporlama süreçlerinde bilgi sistemlerinin kullanılması sürecin genel mantığını değiştirmese de finansal verilerin işlenmesini, saklanmasını, aktarılmasını doğrudan etkilemekte ve iç kontrol ortamının yapısını da değiştirmektedir. Dolayısıyla bu gelişmeler finansal denetimin kapsamını da etkilemiş olup bilgi sistemleri denetimi ile beraber yürütülen finansal denetimin önemi artırmıştır. Diğer bir ifadeyle, finansal denetimin nihai amacı ve kapsamında bir değişiklik olmasa da bilgi sistemlerinin kullanımının artması, faaliyetlerin yürütülme şeklini ve iş süreçlerinin üzerindeki kontrol noktalarını etkilediği gibi denetim sürecini de etkilemiş olmaktadır. Çalışmanın konusunu bağımsız denetçilerin bilgi sistem denetiminin bağımsız denetime etkisine dair görüşleri oluşturmaktadır. Bu bağlamda anketin ikinci bölümüne ait sorular literatürden

faydalanarak hazırlanmış olup, bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşleri tespit edilmeye çalışılmıştır. Ayrıca konuyla ilgili GİB tarafından zorunlu tutulan e-belge özel entegratörleri bilgi sistemleri denetimi klavuzu yayınlanmıştır. Anketin üçüncü bölüm soruları GİB tarafından yayınlanmış olan ve zorunlu tutulan e-Belge özel entegratörleri bilgi sistemleri denetimi klavuzu doğrultusunda hazırlanmış olup bu anket soruları ile bağımsız denetçilerin e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerinin araştırılması amaçlanmaktadır. Bu amaç doğrultusunda Ankara ilinde yer alan bağımsız denetçilere yüz yüze anket uygulamalı bir araştırma yapılmış, elde edilen veriler çeşitli istatistiki yöntemlerle analiz edilmiş, ulaşılan sonuçlar paylaşılmıştır.

Çalışmanın amacı ise bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşlerini ve bağımsız denetçilerin e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerini araştırmaktır. Bu amaç doğrultusunda Ankara ilinde faaliyet gösteren bağımsız denetim kuruluşlarında farklı ünvanlar altında görev yapan KGK tarafından yetkilendirilen (sorumlu ortak baş denetçi, baş denetçi, kıdemli denetçi, denetçi yardımcısı, denetçi) bağımsız denetçilere konuyla ilgili farkındalıklarını ve bakış açılarını anlamak için yüz yüze anket uygulamalı bir araştırma yapılmıştır.

Elde edilen sonuçlar ışığında, bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi hakkında görüşleri doğrultusunda önerilerde bulunulmuştur.

3.2. Araştırmanın Evreni ve Örneklemi

Çalışma evrenini Ankara ilinde faaliyet gösteren bağımsız denetim kuruluşlarında görev yapan bağımsız denetçiler oluşturmaktadır. KGK'dan alınan verilere göre Ankara ilinde toplamda 2472 kayıtlı bağımsız denetçi olup faal bağımsız denetçilerin sayısı 612 gayri faal bağımsız denetçi sayısı 1860'dır.

Araştırma kapsamında Ankara ilinde bağımsız denetim kuruluşlarında faaliyet gösteren 120 bağımsız denetçiye anket uygulanmıştır.

3.3. Araştırmanın Veri Toplama Yöntemi

Bu araştırmada verilerin toplanabilmesi için beşli likert ölçeği ile anket tekniği kullanılmıştır. Bir veri toplama aracı olarak anket, katılımcıların belirli bir konuda düşünce, tutum ve davranışlarını daha önce belirlenmiş bir sırada ve yapıda oluşturulmuş sorulara dayalı olarak elde etmeyi sağlamaktadır. Anket sosyal bilimlerde en fazla kullanılan veri toplama aracıdır. Çünkü anket yoluyla elde edilen verilerin, istatistiksel ve matematiksel analizlerden geçirilmesi kolaydır. Böylece katılımcıların araştırılan konuda düşünce, tutum ve görüşlerini belirlemek, çeşitli çıkarımlarda bulunmak ve karşılaştırmalar yapmak mümkün olabilmektedir (Gürbüz ve Şahin, 2016: 179).

Anket formu katılımcılara hitaben yazılmış bir ön bilgi yazısı ile başlamakta ve üç ana bölümden meydana gelmektedir. Anketin birinci bölümünde katılımcıların demografik özelliklerini tespit etmeye yönelik 9 adet soru yer almaktadır. Anketin ikinci bölümünde katılımcıların bilgi sistemleri denetimi ve bağımsız denetim ile ilgili ifadelerle katılma düzeylerine dair hazırlanan sorulara vermiş oldukları cevapları ölçmeye yönelik 16 adet soru yer almaktadır. Bu sorulara verilecek cevaplar, “1- Kesinlikle Katılmıyorum, 2-Katılmıyorum, 3-Kararsızım, 4-Katılıyorum ve 5- Kesinlikle Katılıyorum” ifadelerinden oluşan 5’li Likert Ölçeği şeklinde hazırlanmıştır. Anketin üçüncü bölümünde e-Belge özel entegratör bilgi sistem denetimi ile ilgili ifadelerle katılma düzeylerine yönelik 33 adet soru yer almaktadır. Bu sorular GİB tarafından yayınlanmış e-belge özel entegratörleri bilgi sistemleri denetimi kılavuzu’nda bulunan ÖEBSD değerlendirme sınıflarında yer alan sorulardan faydalanılarak, “1-Kesinlikle Katılmıyorum, 2-Katılmıyorum, 3-Kararsızım, 4-Katılıyorum ve 5-Kesinlikle Katılıyorum” ifadelerinden oluşan 5’li Likert Ölçeği şeklinde hazırlanmıştır. 5’li likert ölçeğine göre hazırlanan anket formundaki ifadelerin yanıtlarının değerlendirilmesi için Tablo 3.1’deki aralıklar kullanılmıştır. Aralıkların eşit olduğu varsayımından hareket edilerek, aritmetik ortalamalar için puan aralığı; 0,80 olarak bulunmuştur.

Tablo 3.1: Aritmetik Ortalamaların Değerlendirme Aralığı

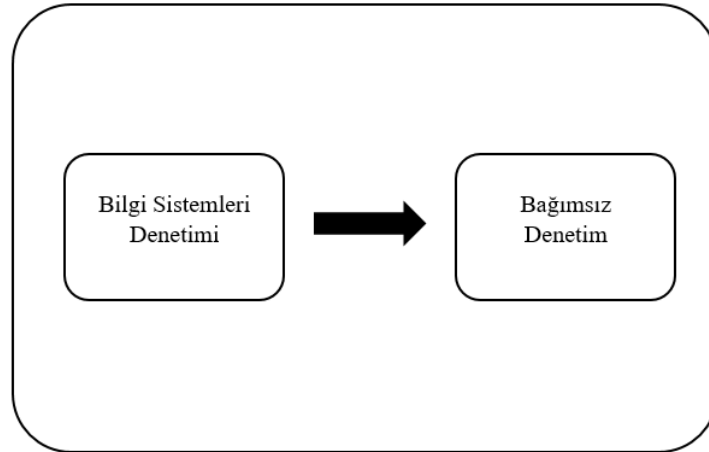
Aralık	Seçenek
00-1,80	Kesinlikle Katılmıyorum
1,81-2,60	Katılmıyorum
2,61-3,40	Kararsızım
3,41-4,20	Katılıyorum
4,21-5,00	Kesinlikle Katılıyorum

Anketlerin bir kısmı denetim şirketlerine elektronik ortamda gönderilmiştir, bir kısmı ise denetim şirketlerinin bire bir ziyaret edilmesi suretiyle, yüz yüze görüşme tekniği kullanılarak yapılmıştır. Anket tekniği uygulaması sonucunda toplam 120 bağımsız denetçiden elde edilen veriler değerlendirmeye alınmıştır.

3.4. Araştırmanın Teorik Modeli ve Hipotezler

Bilgi sistemleri denetiminin bağımsız denetime etkisini ölçmek üzere oluşturulan temel model Şekil 3.1’de gösterilmiştir.

Şekil 3.1: Araştırmanın Temel Modeli



Çalışmanın modelinin belirlenmesinde daha önceden yapılmış olan ampirik çalışmalar incelenmiş ve araştırmanın modeli, literatürdeki teorik bilgilerinden oluşturulmuştur. Bu kapsamda önceden çalışılmış olan analizlerde oluşturulan ilişkiler esas alınarak model belirlenmiştir.

Araştırmanın amacına yönelik temel hipotezi, “Bilgi sistemleri denetimi ile bağımsız denetim arasındaki ilişki anlamlıdır”, şeklindedir.

Araştırmada irdelenen hipotezler aşağıda verilmiştir.

H₁: Bilgi sistem denetimi ile bağımsız denetim arasında anlamlı bir ilişki vardır.

H₂: Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri cinsiyetlerine göre farklılaşmaktadır.

H₃: Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H₄: Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri yaş durumuna göre farklılaşmaktadır.

H₅: Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri eğitim durumuna göre farklılaşmaktadır.

H₆: Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H₇: Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H₈: Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri yüksektir.

H₉: Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H_{9.1}: Bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H_{9.2}: Bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H_{9.3}: Bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H_{9.4}: Bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H9.5: Bağımsız denetçilerin ÖEBSĐ deęerlendirme sınıflarından erişim güvenlięi ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H9.6: Bağımsız denetçilerin ÖEBSĐ deęerlendirme sınıflarından iş süreklilięi, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H9.7: Bağımsız denetçilerin ÖEBSĐ deęerlendirme sınıflarından denetim izleri yönetimi raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H9.8: Bağımsız denetçilerin ÖEBSĐ deęerlendirme sınıflarından deęişiklik yönetimi raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H9.9: Bağımsız denetçilerin ÖEBSĐ deęerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H9.10: Bağımsız denetçilerin ÖEBSĐ deęerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.

H10: Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.1: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.2: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.3: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından personelin nitelięi ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.4: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.5: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından erişim güvenlięi raporu ile ilgili ifadelere ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.6: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iş süreklilięi, risk yönetimi ve acil durum planları raporu ile ilgili ifadelere ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.7: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından denetim izleri yönetimi raporu ile ilgili ifadelere ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.8: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından deęişiklik yönetimi raporu ile ilgili ifadelere ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.9: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi raporu ile ilgili ifadelere ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H10.10: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller raporu ile ilgili ifadelere ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.

H11: Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.

H11.1: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.

H11.2: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelere ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.

H11.3: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından personelin nitelięi ile ilgili ifadelere ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.

H11.4: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelere ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.

H11.5: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından erişim güvenlięi ile ilgili ifadelere ilişkin bilgi düzeyleri yař durumuna göre farklılaşmaktadır.

H11.6: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iş süreklilięi, risk yönetimi ve acil durum planları raporu ile ilgili ifadelere ilişkin bilgi düzeyleri yař durumuna göre farklılaşmaktadır.

H11.7: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelere ilişkin bilgi düzeyleri yař durumuna göre farklılaşmaktadır.

H11.8: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından deęişiklik yönetimi ile ilgili ifadelere ilişkin bilgi düzeyleri yař durumuna göre farklılaşmaktadır.

H11.9: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelere ilişkin bilgi düzeyleri yař durumuna göre farklılaşmaktadır.

H11.10: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller raporu ile ilgili ifadelere ilişkin bilgi düzeyleri yař durumuna göre farklılaşmaktadır.

H12: Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H12.1: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H12.2: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelere ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H12.3: Bağımsız denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Personelin Nitelięi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.

H12.4: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelere ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H12.5: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından erişim güvenlięi ile ilgili ifadelere ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H_{12.6}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H_{12.7}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H_{12.8}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H_{12.9}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H_{12.10}: Bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.

H₁₃: Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H_{13.1}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H_{13.2}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerle ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H_{13.3}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H_{13.4}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H_{13.5}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelerle ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H13.6: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme Sınıflarından İş Süreklilięi, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.

H13.7: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H13.8: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından deęişiklik yönetimi raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H13.9: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H13.10: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.

H14: Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H14.1: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H14.2: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H14.3: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından personelin nitelięi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H14.4: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H14.5: Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından erişim güvenlięi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H_{14.6}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H_{14.7}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H_{14.8}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H_{14.9}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

H_{14.10}: Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.

3.5. Araştırmanın Sınırlılıkları

Bu çalışmanın bazı sınırlılıkları mevcuttur. Bunlar aşağıdaki gibi sıralanabilir.

- Çalışmanın evreni bakımından: Araştırmanın takvimi, bütçesi ve kaynakları gibi kısıtları nedeniyle çalışma evreni Ankara ili ile sınırlıdır.
- Bağımsız denetçilerin çalışma durumu bakımından: Ankara ilinde faaliyet gösteren bağımsız denetim şirketlerinde aktif olarak çalışanlarla sınırlıdır.
- Veri toplama tekniği bakımından: Araştırma anket tekniği ile sınırlıdır.
- Konu bakımından: Bu çalışma bilgi sistemleri denetiminin bağımsız denetime etkisi ile sınırlıdır.

3.6. Araştırma Verilerinin Analizi

Verilerin analizi IBM SPSS sürüm 26.0 istatistik programı (Chicago, IL, ABD) kullanılarak yapılmıştır. Verilerin dağılımının normalliğini test etmek için basıklık ve çarpıklık değerlerine bakılmıştır. Betimleyici istatistikler ortalama (\bar{X}), standart sapma

(S) ve yüzdeler (%) olarak verilmiştir. Normal dağılıma uyduğu belirlenen gruplar arasındaki anlamlı farklılıkların analizi, iki gruptan oluşanlar için bağımsız örneklem t testi, üç veya daha fazla gruptan oluşanlar için tek yönlü varyans analizi kullanılarak yapılmıştır. Varyans analizinde anlamlı farklılıkların hangi gruplar arasında olduğunu belirlemek için post hoc çoklu karşılaştırmalardan Tukey in HSD testi kullanılmıştır. $p < 0,05$ değeri istatistiksel olarak anlamlı kabul edilmiştir.

Ölçeğin güvenilirliği için Cronbach's Alpha iç tutarlılık katsayısına bakılmıştır. Ölçeğin Cronbach's Alpha iç tutarlılık katsayısı 0,935 olarak tespit edilmiştir. Maddelerin ayırt ediciliklerini belirlemek amacıyla madde-ölçek korelasyonuna bakılmıştır. Bu doğrultuda, kullanmış olduğumuz ölçeğin madde-ölçek korelasyonları incelenmiş olup değerlerinin 0,258 ile 0,963 arasında değiştiği görülmüştür.

Veri setinin faktör analizi için uygun olup olmadığını belirlemek amacıyla Kaiser-Meyer-Olkin'in (KMO) ve Barlett Küresellik testlerine bakılmıştır. Yapılan analiz sonucu Kaiser-Meyer-Olkin katsayısı (KMO değeri 0,768) ve Barlett Küresellik testi ($\chi^2(1176)=4215,829$; $p < 0,001$) değeri faktör analizi için uygun olduğunu göstermektedir.

Yapılan açımlayıcı faktör analizi sonucunda, ölçeğin faktör özdeğeri 1'den büyük 14 faktör içerdiği ortaya çıkmıştır. Varimax rotasyonu ile elde edilen bu 14 faktörlü yapı toplam varyansın yüzde 70'ini açıklamaktadır. Toplam 49 maddeden oluşan ölçek maddelerinin faktör yüklerinin 0,413 ile 0,873 arasında değişim gösterdiği tespit edilmiştir. Açımlayıcı faktör analizi sonucunda elde edilen alt boyutların geçerliliğini göstermek üzere doğrulayıcı faktör analizi uygulanmıştır. Doğrulayıcı faktör analizi sonucunda 49 maddelik 14 faktörden oluşan yapının çalışma örnekleme için uygun olduğu bulunmuştur.

3.7. Araştırma Bulguları ve Yorumlar

3.7.1. Sosyo-Demografik Özellikler ile İlgili Bulguların Analizi

Anketin birinci bölümünde yer alan katılımcıların kişisel ve demografik verilerine ait ifadelerle ait frekans ve yüzde analizine ait sonuçlar Tablo 3.2'de verilmiştir.

Tablo 3.2: Sosyo-Demografik Özellikler ile İlgili Bulguların Analizi

	Denetçi Yardımcısı n(%)	Denetçi n(%)	Kıdemli Denetçi n(%)	Baş Denetçi n(%)	Sorumlu Ortak Baş Denetçi n(%)	Toplam n(%)
Cinsiyet						
Kadın	14(11,7%)	14(11,7%)	5(4,2%)	7(5,8%)	4(3,3%)	44(36,7%)
Erkek	15(12,5%)	23(19,2%)	15(12,5%)	10(8,3%)	13(10,8%)	76(63,3%)
Yaşınız						
≤ 30	13(10,8%)	4(3,3%)	4(3,3%)	-	-	21(17,5%)
30-39	4(3,3%)	3(2,5%)	8(6,7%)	-	1(0,8%)	16(13,3%)
40-49	10(8,3%)	19(15,8%)	5(4,2%)	2(1,7%)	6(5,0%)	42(35,0%)
50-59	2(1,7%)	8(6,7%)	2(1,7%)	8(6,7%)	4(3,3%)	24(20,0%)
60 ≥	-	3(2,5%)	1(0,8%)	7(5,8%)	6(5,0%)	17(14,2%)
Öğrenim Durumunuz						
Lisans	14(11,7%)	19(15,8%)	9(7,5%)	9(7,5%)	9(7,5%)	60(50,0%)
Yüksek Lisans	15(12,5%)	14(11,7%)	10(8,3%)	8(6,7%)	6(5,0%)	53(44,2%)
Doktora	-	4(3,3%)	1(0,8%)	-	2(1,7%)	7(5,8%)
Çalışma Süreniz						
1-5 yıl	29(24,2%)	19(15,8%)	2(1,7%)	-	2(1,7%)	52(43,3%)
6-10 yıl	-	15(12,5%)	15(12,5%)	1(0,8%)	1(0,8%)	32(26,7%)
11-15 yıl	-	3(2,5%)	3(2,5%)	3(2,5%)	4(3,3%)	13(10,8%)
16 yıl ve üzeri	-	-	-	13(10,8%)	10(8,3%)	23(19,2%)
E belge Özel entegratör kuruluşları hakkında bilgi sahibi misiniz?						
Evet	12(10,0%)	22(18,3%)	10(8,3%)	17(14,2%)	15(12,5%)	76(63,3%)
Kısmen	9(7,5%)	9(7,5%)	9(7,5%)	-	1(0,8%)	28(23,3%)
Hayır	8(6,7%)	6(5,0%)	1(0,8%)	-	1(0,8%)	16(13,3%)
E Fatura E Defter E Arşiv hakkında bilgi sahibi misiniz?						
Evet	25(20,8%)	35(29,2%)	19(15,8%)	17(14,2%)	16(13,3%)	112(93,3%)
Kısmen	4(3,3%)	2(1,7%)	1(0,8%)	-	-	7(5,8%)
Hayır	-	-	-	-	1(0,8%)	1(0,8%)
Bilgi sistemleri denetçisi sertifikası (CISA)'na sahip misiniz?						
Evet	-	3(2,5%)	4(3,3%)	5(4,2%)	5(4,2%)	17(14,2%)
Hayır	29(24,2%)	34(28,3%)	16(13,3%)	12(10,0%)	12(10,0%)	103(85,8%)

Araştırmaya katılan bağımsız denetçilerin denetim firmasındaki pozisyonlarının dağılımı incelendiğinde; katılımcıların %24,2'sinin denetçi yardımcısı, %30,9'unun

denetçi, %16,7'sinin kıdemli denetçi, %14,1'inin baş denetçi ve %14,1'inin sorumlu ortak baş denetçi olduğu görülmektedir.

Araştırmaya katılan bağımsız denetçilerin cinsiyet değişkeninin dağılımı incelendiğinde; %36,7'sinin kadın, geriye kalan %63,3'nün ise erkek olduğu belirlenmiştir.

Araştırmaya katılan bağımsız denetçilerin yaş aralıkları incelendiğinde; katılımcıların %17,5'inin 30 yaşın altında olduğu, %13,3'ünün 30-39 yaş aralığında, %35'inin 40-49 yaş aralığında, %20'sinin 50-59 yaş aralığında ve %14,2'sinin ise 60 yaş üzeri olduğu görülmektedir.

Araştırmaya katılan bağımsız denetçilerin öğrenim durumları değişkeninin dağılımı incelendiğinde; katılımcıların %50'si lisans mezunu, %44,2'si yüksek lisans mezunu, %5,8'i doktora mezunu olduğu görülmektedir. Buna göre araştırma kapsamında öğrenim durumları açısından lisansüstü eğitim yapanların oranının %50 olması dikkat çekmektedir.

Araştırmaya katılan bağımsız denetçilerin mesleki çalışma süresi değişkeninin dağılımı incelendiğinde; katılımcıların %19,2'si 16 yıl ve üzeri, %10,8'i 11-15 yıl arası, %26,7'si 6-10 yıl arası, %43,3'ü 1-5 yıl arası olduğu görülmektedir.

Araştırmaya katılan bağımsız denetçilerin %63,3'ünün e-belge özel entegratör kuruluşları hakkında bilgi sahibi oldukları, %13,3'ünün ise bilgi sahibi olmadıkları anlaşılmıştır.

Araştırmaya katılan bağımsız denetçilerin %93,3'ünün e-fatura, e-belge, e-arşiv hakkında bilgi sahibi oldukları, %0,8'inin ise bilgi sahibi olmadıkları görülmektedir.

Araştırmaya katılan bağımsız denetçilerin %14,2'sinin bilgi sistemleri denetçi sertifikası (CISA)'na sahip oldukları, %85,8'inin ise bu sertifikaya sahip olmadıkları görülmektedir.

3.7.2. Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşlerinin Analizi

Tablo 3.3'de Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşleri ile ilgili 16 ifade yer almaktadır. Tabloda katılımcılar

tarafından verilen cevapların frekansı, yüzdesi, standart sapması ve ortalamaları verilmektedir.

Tablo 3.3: Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere İlişkin Görüşlerine Ait Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)					Veri Sayısı (n) - (%)	Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum			
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz.								
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1. Bilgi sistemleri denetimi bağımsız denetimin bir parçasıdır, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekir.	2	2	13	79	24	120	4,01	0,728
	1,7	1,7	10,8	65,8	20,0	100		
2. *Bilgi sistemleri denetimi, bağımsız denetçinin muhasebe ve iç kontrol sistemi ile ilgili yeterli bir anlayış edinmek amacıyla izlediği yöntemleri etkilemez.	8	18	18	37	39	120	3,68	1,258
	6,7	15	15,0	30,8	32,5	100		
3. Bağımsız denetimde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeler.	3	4	15	46	52	120	4,17	0,947
	2,5	3,3	12,5	38,3	43,3	100		
4. Bilgi sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkisi vardır.	1	0	18	54	47	120	4,22	0,758
	0,8	0	15,0	45,0	39,2	100		
5. Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.	2	1	6	51	60	120	4,38	0,769
	1,7	0,8	5,0	42,5	50,0	100		

* Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere İlişkin Görüşlerine Ait ifadelerinden 2,7,8,13* ters ifadelerdir. Ters ifadeler analize alınırken SPSS programı üzerinde "Recode into Same Variables" komutu kullanılarak yeniden kodlanmıştır

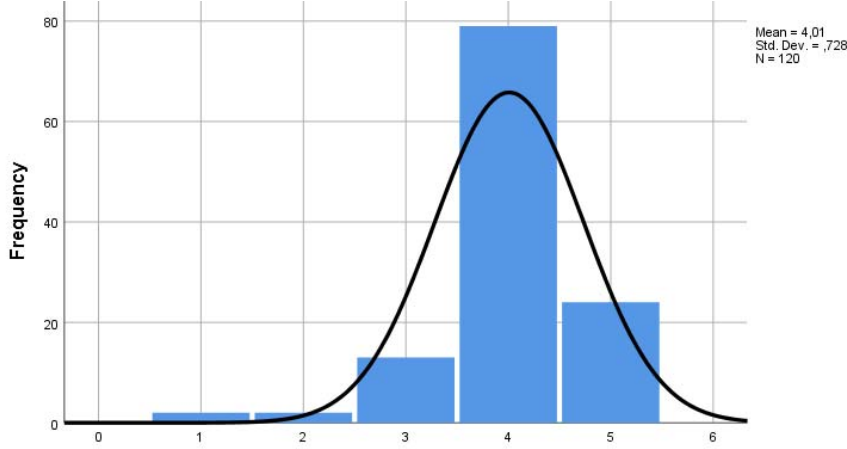
6. Bilgi sistemlerindeki altyapı yetersizlikleri ve performans sorunlarının bağımsız denetim üzerine etkisi vardır.	1	3	9	67	40	120		
	0,8	2,5	7,5	55,8	33,3	100	4,18	0,745
7. *Bilgi sistemleri kontrol ve denetim faaliyetlerinin yetersizliğinin bağımsız denetime etkisi yoktur.	3	11	10	41	55	120		
	2,5	9,2	8,3	34,2	45,8	100	4,12	1,063
8. *Bilgi sistemlerindeki veri ve programlara yetkisiz erişimin bağımsız denetim üzerinde etkisi yoktur.	4	8	14	41	53	120		
	3,3	6,7	11,7	34,2	44,2	100	4,09	1,061
9. Denetim planı oluşturulurken, denetim riskinin büyüklüğü belirlenirken bilgi sistem denetimi sonuçları dikkate alınmalıdır.	1	0	1	67	45	120		
	0,8	0	5,8	55,8	37,5	100	4,29	0,653
10. Bilgi sistemleri denetiminin de iç kontrol ve denetim mekanizmaları değerlendirmelerinin bağımsız denetim kanıt güvenilirliğine etkisi vardır.	0	1	7	56	56	120		
	0	0,8	5,8	46,7	46,7	100	4,39	0,639
11. Bilgi sistemleri denetimi şirket verilerine erişimi sınırlandırarak yasalara ve muhasebe standartlarına uyumu geliştirir, kontrolleri iyileştirir.	4	9	26	44	37	120		
	3,3	7,5	21,7	36,7	30,8	100	3,84	1,053
12. Bilgi sistemleri üzerine siber saldırıların bağımsız denetim üzerinde olumsuz etkisi vardır.	2	6	11	58	43	120		
	1,7	5,0	9,2	48,3	35,8	100	4,12	0,891
13. *Bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki etmez.	3	9	15	54	39	120		
	2,5	7,5	12,5	45,0	32,5	100	3,98	0,991

14. Bağımsız denetçi, bilgi sistemlerinin içyapısında bulunan önemli olarak değerlendirilebilecek hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır.	0	7	14	50	49	120		
							4,18	0,857
	0	5,8	11,7	41,7	40,8	100		
15. Finansal tablolara kaynak verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.	0	1	6	64	49	120		
							4,34	0,615
	0	0,8	5,0	53,3	40,8	100		
16. Bilgi Sistemleri Denetimi üzerine bağımsız denetçilere zorunlu eğitim verilmelidir.	0	5	11	55	49	120		
	0	4,2	9,2	45,8	40,8	100	4,23	0,786
Ölçeğin Ortalaması ve Standart Sapması							4,02	0,441

Tablo 3.3’de görüldüğü üzere bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşleri ile ilgili ifadelere katılımcıların (1- Kesinlikle Katılmıyorum ve 5-Kesinlikle Katılıyorum aralığında) verdikleri yanıtlar analiz edilmiş ve sonuçlara ulaşılmıştır.

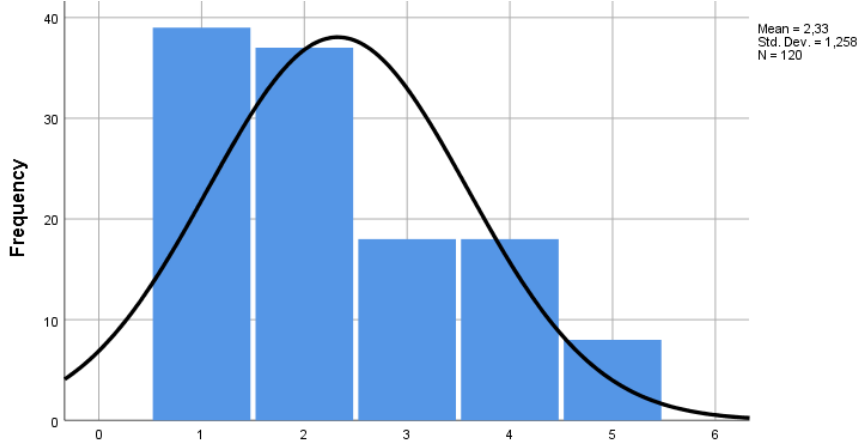
Araştırmaya katılan bağımsız denetçilerin “Bilgi sistemleri denetimi bağımsız denetimin bir parçasıdır, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekir.” ifadesine %65,8 oranında katıldığı, %20 oranında ise kesinlikle katıldığı görülmektedir. İfadenin ortalamasının ($\bar{X}=4,01$ “katılıyorum”) yüksek değer aralığında olduğu belirlenmiştir. Buna göre, katılımcıların büyük kısmı (%85,8) bilgi sistemleri denetiminin bağımsız denetimin bir parçası olduğunu bildiklerini, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerektiğini belirtmektedirler.

Şekil 3.2: Bilgi sistemleri denetimi bağımsız denetimin bir parçasıdır, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekir.



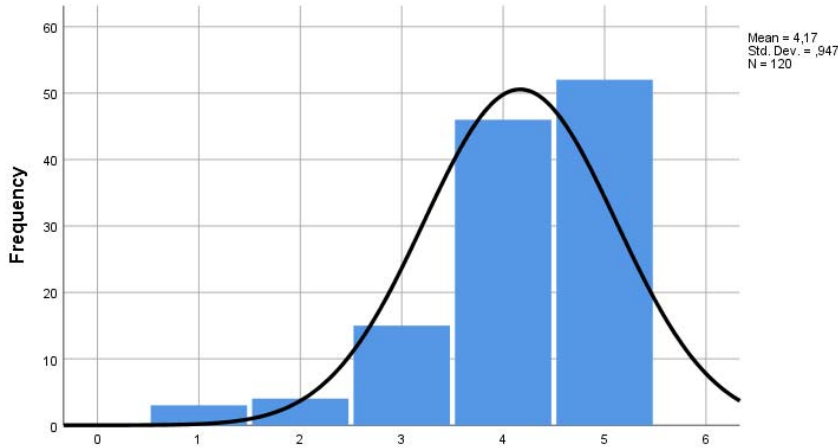
Katılımcılara Tablo 3.3'deki 2. soruda bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşleri ile ilgili ters bir formatta “Bilgi sistemleri denetimi, bağımsız denetçinin muhasebe ve iç kontrol sistemi ile ilgili yeterli bir anlayış edinmek amacıyla izlediği yöntemleri etkilemez.” ifadesi sunulmuştur. Katılımcıların %63,3'ü bu ifadeye katılmadıklarını yani bilgi sistemleri denetiminin, bağımsız denetçinin muhasebe ve iç kontrol sistemi ile ilgili yeterli bir anlayış edinmek amacıyla izlediği yöntemleri etkileyeceğini düşünmektedirler. İfadenin ters kodlanmış şekilde ortalaması ($\bar{X}=3,68$) olup bu durum da katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediğini göstermektedir. Standart sapma değeri açısından bu ifade, bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadeler katılma düzeyi ifadelerinden en yüksek değere ($SS=1,258$) sahip olduğu görülmektedir. Bu fikrin tam tersini savunan (%21,7) tarafın da dikkate alınması gereken çoğunluğa sahip olduğu önemli bir durumdur.

Şekil 3.3: Bilgi sistemleri denetimi, bağımsız denetçinin muhasebe ve iç kontrol sistemi ile ilgili yeterli bir anlayış edinmek amacıyla izlediği yöntemleri etkilemez.



“Bağımsız denetimde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeler.” İfadesine katılımcıların %38,3’ü katılıyorum, %43,3’ü kesinlikle katılıyorum, %12,5’i kararsız kalmış, %5,8’i ise katılmamıştır. İfadenin ortalamasının ($\bar{X}=4,17$) “katılıyorum” değer aralığında olduğu tespit edilmiştir. Buna göre, bağımsız denetimde bilgi sistemlerinin üzerinde durulmamasının denetimin gerçekleştirilme amacı olan makul güvenceyi zedelediği anlaşılmaktadır.

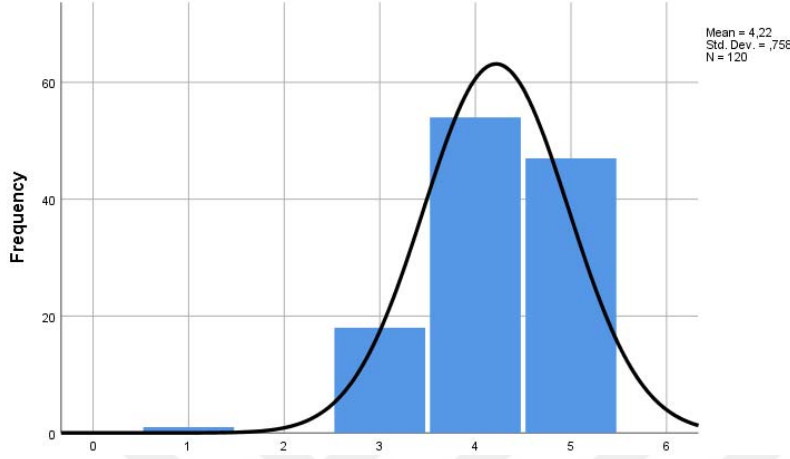
Şekil 3.4: Bağımsız denetimde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeler.



“Bilgi sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkisi vardır.” ifadesine katılımcıların %84,2 oranı ile (%39,2=kesinlikle katılıyorum, %45,0=katılıyorum) büyük çoğunluğunun katıldığı sadece %0,8’inin katılmadığı ve %15’ininde kararsız olduğu görülmektedir. İfadeye ait ortalama ($\bar{X}=4,22$ “kesinlikle katılıyorum”) en yüksek değere sahiptir. Buna göre, katılımcılar bilgi

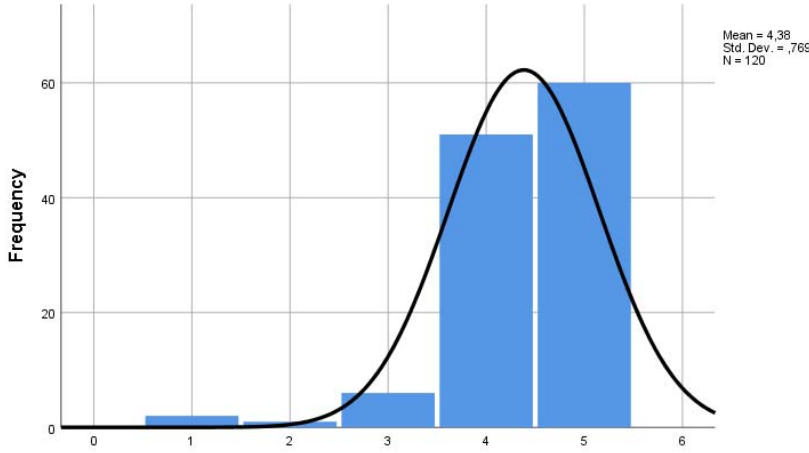
sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkiye sahip olduğunu belirtmektedirler.

Şekil 3.5: Bilgi sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkisi vardır.



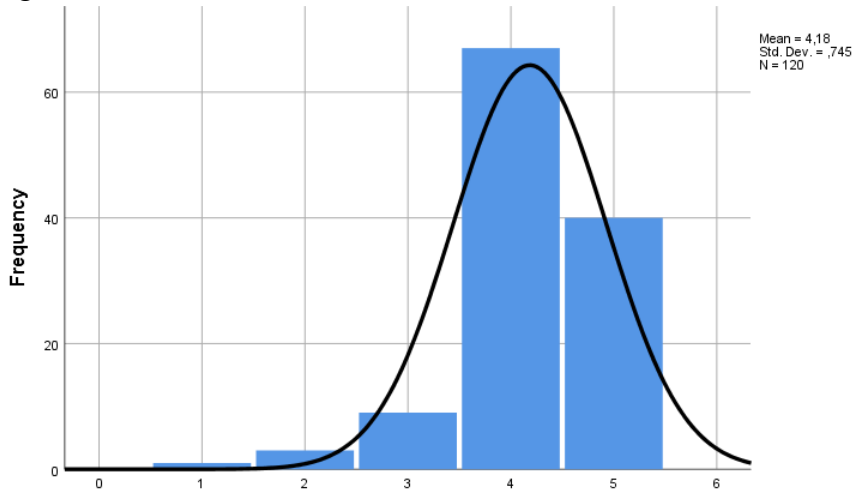
Araştırmaya katılan katılımcıların çok büyük bir kısmının (%92,5) “Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.” ifadesine katıldığı (%42,5=katılıyorum, %50,0=kesinlikle katılıyorum), %5’inin kararsız kaldığı ve sadece %2,5’inin ise katılmadığı (%0,8=katılmıyorum, %1,7=kesinlikle katılmıyorum) görülmektedir. Bu ifadenin ortalaması ($\bar{X}=4,38$) bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşleri ile ilgili ifadelerinin en yüksek ortalamasına sahip olduğu ve ifadenin “kesinlikle katılıyorum” değeri aralığında olduğu görülmektedir. Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışmasının daha şeffaf sonuçların ortaya konmasına katkı sağlayacağı neredeyse tüm katılımcılar tarafından ifade edilmektedir.

Şekil 3.6: Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.



Katılımcılara “Bilgi sistemlerindeki altyapı yetersizlikleri ve performans sorunlarının bağımsız denetim üzerine etkisi vardır” ifadesi sunulmuş, %89,1’i katıldığını (%55,8=katılıyorum, %33,3=kesinlikle katılıyorum), %3,3’ü katılmadığını (%2,5=katılmıyorum, %0,8=kesinlikle katılmıyorum), %7,5’i ise kararsız kaldığını belirtmişlerdir. İfadenin ortalaması ($\bar{X}=4,18$ “katılıyorum”) yüksek bir değer aralığında olduğu tespit edilmiştir. Bu ifadenin standart sapma değeri ($SS=0,745$) oldukça düşük bir değerdir.

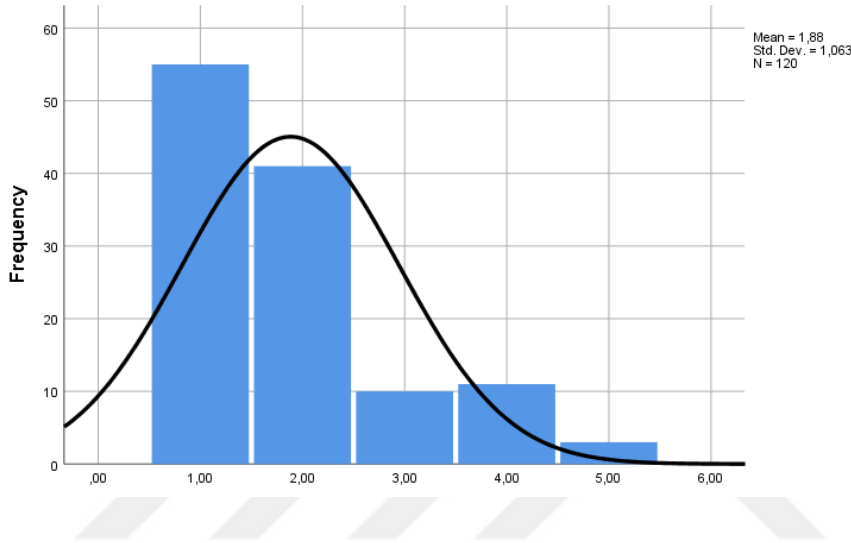
Şekil 3.7: Bilgi sistemlerindeki altyapı yetersizlikleri ve performans sorunlarının bağımsız denetim üzerine etkisi vardır.



Katılımcılara, kontrol denetim faaliyetleri ile ilgili ters bir formatta “Bilgi sistemleri kontrol ve denetim faaliyetlerinin yetersizliğinin bağımsız denetime etkisi yoktur.” ifadesi sunulmuştur. Katılımcıların %80’i bu ifadeye katılmadıklarını yani bilgi sistemleri

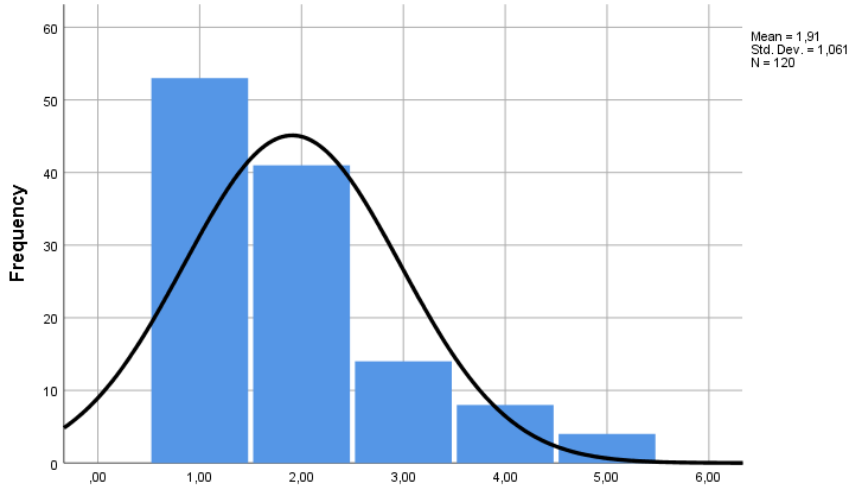
kontrol ve denetim faaliyetlerinin yetersizliğinin bağımsız denetime etkisi olduğunu ifade etmişlerdir. Ancak katılımcıların %11,7'si söz konusu yetersizliğin bağımsız denetime etkisi olmadığını belirtmişlerdir. Bu ifadenin ters kodlanmış şekilde ortalamasının (\bar{X} =4,12 “katılıyorum”) yüksek bir değer aralığında olduğu görülmektedir. Ayrıca bu ifadenin SS=1,063 standart sapma değerine sahip olduğu görülmektedir.

Şekil 3.8: Bilgi sistemleri kontrol ve denetim faaliyetlerinin yetersizliğinin bağımsız denetime etkisi yoktur



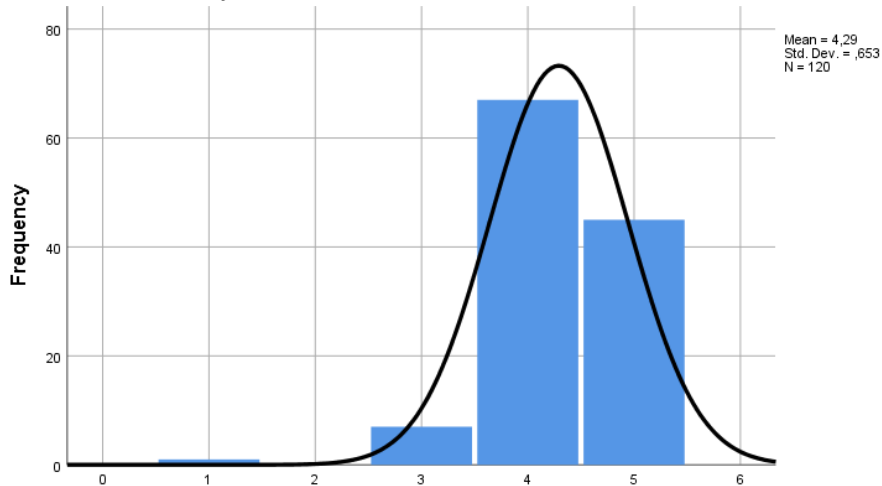
Bilgi sistemlerindeki veri ve programlara yetkisiz erişimin önemli olduğu düşünülmüş ve bu bağlamda katılımcılara ters formatta “Bilgi sistemlerindeki veri ve programlara yetkisiz erişimin bağımsız denetim üzerinde etkisi yoktur.” ifadesi sunulmuştur. Katılımcıların %78,4’ü bu ifadeye katılmadıklarını (%34,2=katılmıyorum, %44,2=kesinlikle katılmıyorum), %10’u katıldıklarını (%6,7=katılıyorum, %3,3=kesinlikle katılıyorum), %11,7’si ise kararsız kaldıklarını belirtmişlerdir. Bu ifadenin olumlu formatının ortalamasının (\bar{X} =4,09 “katılıyorum”) yüksek bir değer aralığında olduğu belirlenmiştir. Böylece, katılımcıların çoğunun bilgi sistemlerindeki veri ve programlara yetkisiz erişimin bağımsız denetim üzerinde etkisinin olduğu fikrinde oldukları söylenebilir.

Şekil 3.9: Bilgi sistemlerindeki veri ve programlara yetkisiz erişimin bağımsız denetim üzerinde etkisi yoktur.



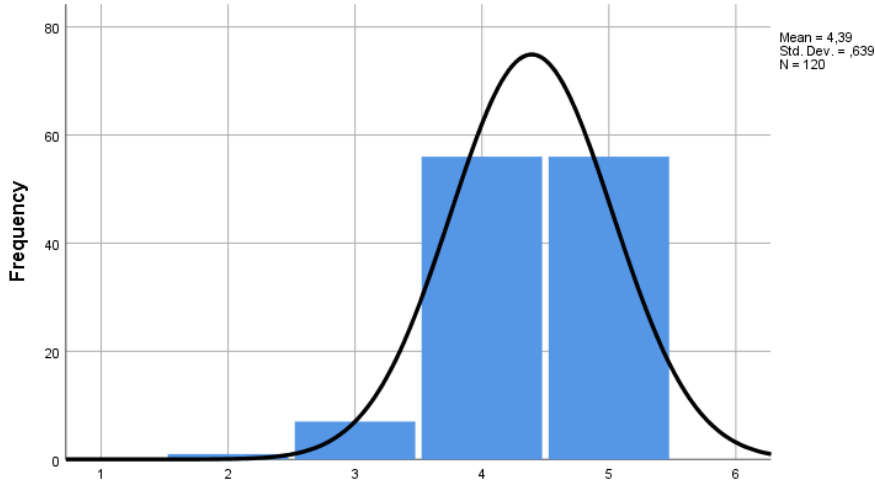
“Denetim planı oluşturulurken, denetim riskinin büyüklüğü belirlenirken bilgi sistemleri denetimi sonuçları dikkate alınmalıdır.” ifadesine bağımsız denetçilerin büyük bir kısmının %93,3’ünün (%55,8= katılıyorum, %37,5=kesinlikle katılıyorum) katıldığı %5,8’lik kısmının kararsız olduğu ve %0,8 kısmının katılmadığı belirlenmiştir. Bu sonuca göre; denetim planı oluşturulurken ve denetim riskinin büyüklüğü belirlenirken bilgi sistemleri denetimi sonuçları dikkate alınmalıdır fikri bağımsız denetçilerin çok büyük bir kısmı tarafından desteklenmektedir. İfadenin ortalamasının ($\bar{X}=4,29$ “kesinlikle katılıyorum”) çok yüksek bir değer aralığında olduğu tespit edilmiştir. Bu ifadenin standart sapma değeri ($SS=0,653$) oldukça düşük bir değerdir.

Şekil 3.10: Denetim planı oluşturulurken, denetim riskinin büyüklüğü belirlenirken bilgi sistem denetimi sonuçları dikkate alınmalıdır.



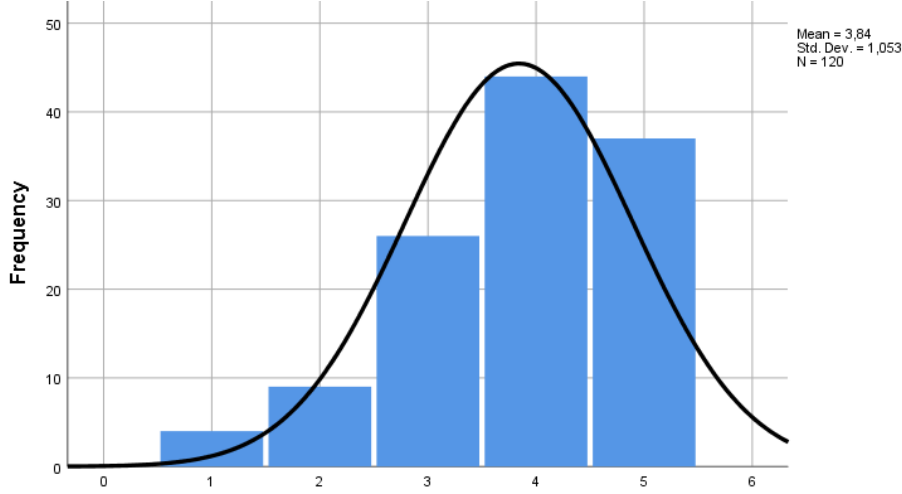
Katılımcılara “Bilgi sistemleri denetimin de iç kontrol ve denetim mekanizmaları değerlendirmelerinin bağımsız denetim kanıt güvenilirliğine etkisi vardır.” ifadesi sunulmuş, %93,4’ü katıldığını (%46,7=katılıyorum, %46,7=kesinlikle katılıyorum), %0,8’i katılmadığını (%0,8=katılmıyorum), %5,8 ’i ise kararsız kaldığını belirtmişlerdir. İfadenin ortalamasının (\bar{X} =4,39 “kesinlikle katılıyorum”) çok yüksek bir değer aralığında olduğu tespit edilmiştir. Bu ifadenin standart sapma değeri SS=0,639’dur.

Şekil 3.11: Bilgi sistemleri denetimin de iç kontrol ve denetim mekanizmaları değerlendirmelerinin bağımsız denetim kanıt güvenilirliğine etkisi vardır.



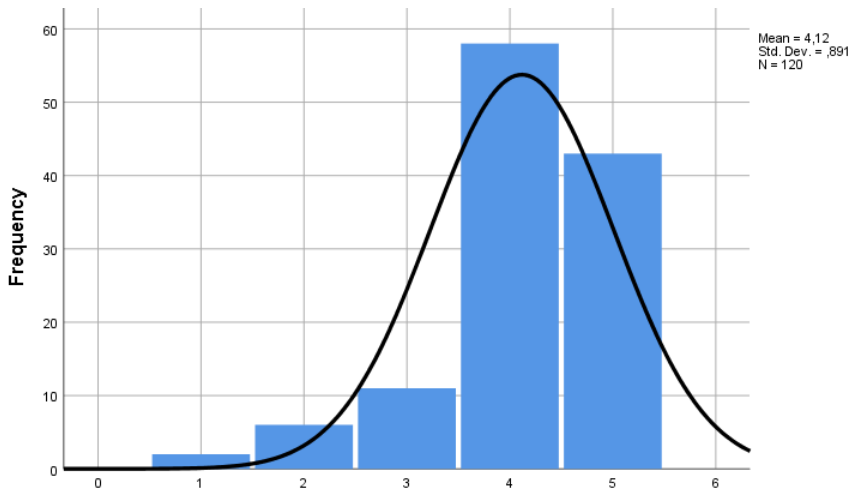
Katılımcılara şirket verilerine erişimi sınırlama ile ilgili olarak sunulan; “Bilgi sistemleri denetimi şirket verilerine erişimi sınırlayarak yasalara ve muhasebe standartlarına uyumu geliştirir, kontrolleri iyileştirir.” ifadesine katılımcıların önemli bir çoğunluğunun (%67,5) katıldıklarını (%36,7=katılıyorum, %30,8=kesinlikle katılıyorum), %21,7’si kararsız kaldıklarını ve geriye kalan %10,8’i ise katılmadıklarını (%7,5=katılmıyorum, %3,3=kesinlikle katılmıyorum) belirtmişlerdir. Bu ifadenin aritmetik ortalamasının (\bar{X} =3,84 “katılıyorum”) yüksek bir değer aralığında olduğu görülmektedir. Bu veriler katılımcıların büyük bir çoğunluğunun, bilgi sistemleri denetiminin şirket verilerine erişimi sınırlamasının yasalara ve muhasebe standartlarına uyumu geliştireceğini ve kontrolleri iyileştireceğini düşündüğünü göstermektedir.

Şekil 3.12: Bilgi sistemleri denetimi şirket verilerine erişimi sınırlayarak yasalara ve muhasebe standartlarına uyumu geliştirir, kontrolleri iyileştirir.



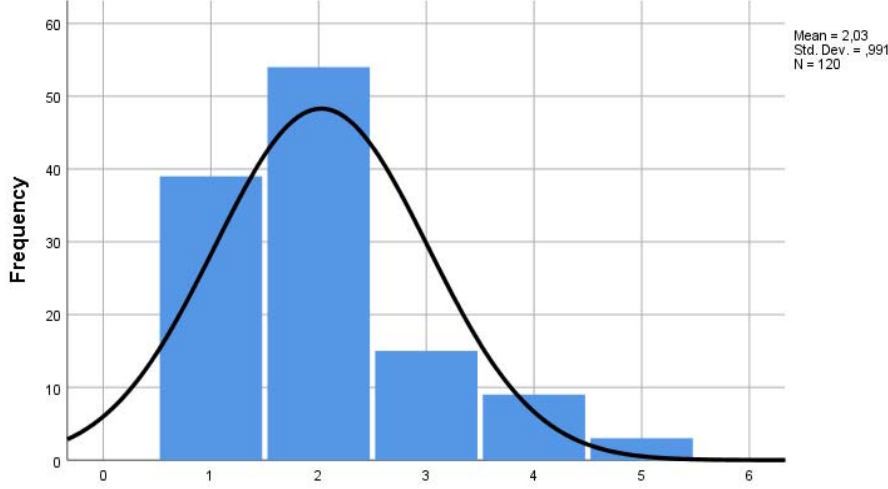
Katılımcılara siber saldırılar ile ilgili sunulan; “Bilgi sistemleri üzerine siber saldırıların bağımsız denetim üzerinde olumsuz etkisi vardır.” ifadesine katılımcıların çok büyük bir çoğunluğu (%84,1) katıldıklarını (%48,3=katılıyorum, %35,8=kesinlikle katılıyorum), %9,2’si kararsız kaldıklarını ve geriye kalan %6,7’si ise katılmadıklarını (%5,0=katılmıyorum, %1,7=kesinlikle katılmıyorum) belirtmişlerdir. Bu ifadenin aritmetik ortalamasına bakıldığında ($\bar{X}=4,12$ “katılıyorum”) yüksek bir değer aralığında olduğu görülmektedir. Bu bağlamda, bilgi sistemleri üzerine siber saldırıların bağımsız denetimin üzerinde olumsuz etkisi olacağı fikri bağımsız denetçiler tarafından benimsenmektedir.

Şekil 3.13: Bilgi sistemleri üzerine siber saldırıların bağımsız denetim üzerinde olumsuz etkisi vardır.



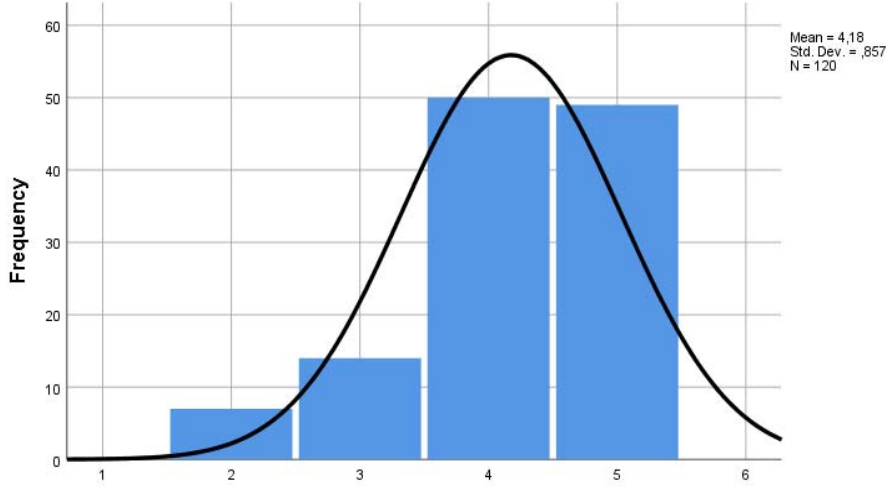
Katılımcılara ters bir formatta “Bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki etmez.” ifadesi sunulmuştur. Katılımcıların %77,5’i bu ifadeye katılmadıklarını yani bilgi sistemlerinin söz konusu verileri doğru üretip üretmediğinin bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki edeceğini düşünmektedirler. İfadenin ters kodlanmış şekilde ortalaması ($\bar{X}=3,98$) olup bu durum katılımcıların bu ifadenin olumlu formatına “katılıyorum” dediğini göstermektedir. Standart sapma değeri $SS=0,991$ olduğu görülmektedir. Bu fikrin tam tersini savunan %10’luk kısmında dikkat çekici olduğu ifade edilebilir.

Şekil 3.14: Bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki etmez.



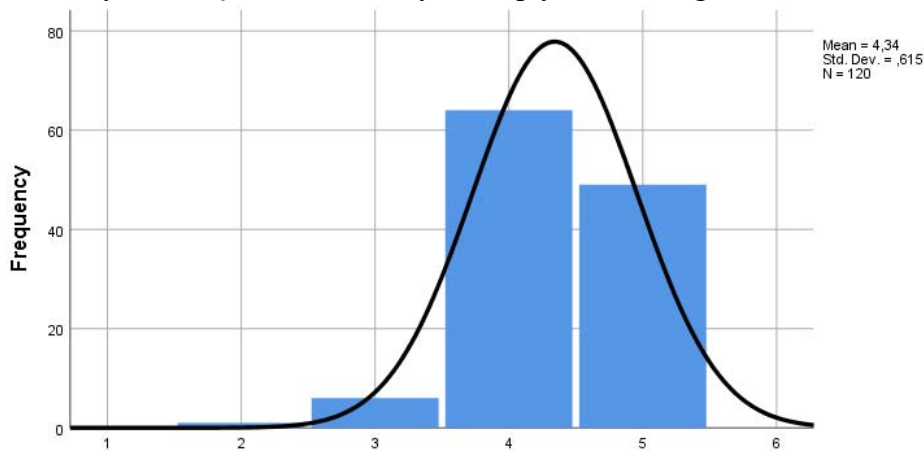
“Bağımsız denetçi, bilgi sistemlerinin iç yapısında bulunan önemli olarak değerlendirilebilecek hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır.” ifadesine katılımcıların çok büyük bir çoğunluğu (%82,5) katıldıklarını (%41,7=katılıyorum, %40,8=kesinlikle katılıyorum), %11,7’si kararsız kaldıklarını ve geriye kalan %5,8’i ise katılmadıklarını (%5,8=katılmıyorum, %0=kesinlikle katılmıyorum) belirtmişlerdir. İfadenin aritmetik ortalamasınının ($\bar{X}=4,18$ “katılıyorum”) yüksek değer aralığında olduğu görülmektedir. Buna göre, katılımcılar; bağımsız denetçi, bilgi sistemlerinin iç yapısında bulunan önemli olarak değerlendirilebilecek hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır fikrini savunmaktadırlar.

Şekil 3.15: Bağımsız denetçi, bilgi sistemlerinin içyapısında bulunan önemli olarak değerlendirilebilecek hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır.



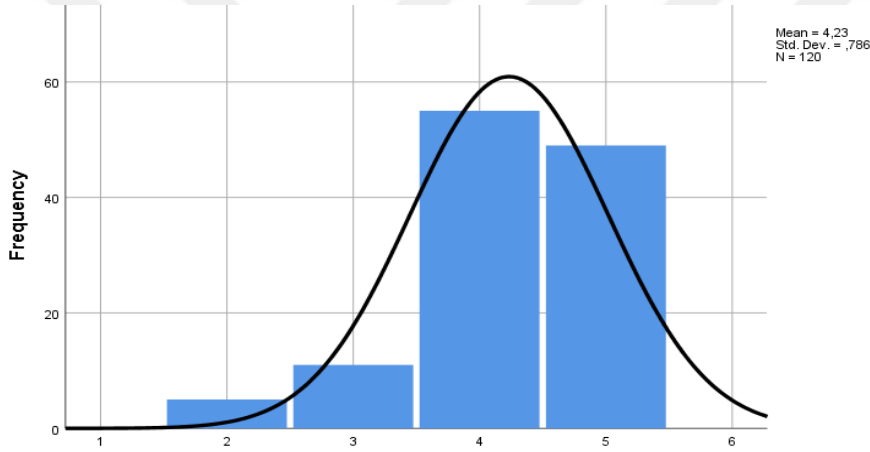
“Finansal tablolara kaynak verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.” ifadesine katılımcıların büyük çoğunluğunun (%94,1) katıldıklarını (%53,3=katılıyorum, %40,8=kesinlikle katılıyorum), %5’i kararsız kaldıklarını ve geriye kalan sadece %0,8’lik kısmı ise katılmadıklarını (%0,8=katılmıyorum, %0=kesinlikle katılmıyorum) belirtmişlerdir. İfadenin aritmetik ortalamasının ($\bar{X}=4,34$ “kesinlikle katılıyorum”) en yüksek bir değer aralığında olduğu görülmektedir. Bu ifadenin standart sapma değeri ise $SS=0,615$ ’dir.

Şekil 3.16: Finansal tablolara kaynak verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.



Bilgi sistemleri denetimi üzerine bağımsız denetçilere zorunlu eğitim verilmesi gibi çözüm önerisi olarak sunulan; “Bilgi sistemleri denetimi üzerine bağımsız denetçilere zorunlu eğitim verilmelidir.” ifadesine katılımcıların tamamına yakını (%86,6) katıldıklarını (%45,8=katılıyorum, %40,8=kesinlikle katılıyorum), %9,2’si kararsız kaldıklarını ve geriye kalan %4,2’si ise katılmadıklarını (%4,2=katılmıyorum, %0=kesinlikle katılmıyorum) belirtmişlerdir. İfadenin aritmetik ortalamasının ($\bar{X}=4,23$ “kesinlikle katılıyorum”) en yüksek değer aralığında olduğu görülmektedir. Buna göre, katılımcıların tamamına yakını bilgi sistemleri denetimi üzerine bağımsız denetçilere zorunlu eğitim verilmelidir fikrini desteklemektedirler.

Şekil 3.17: Bilgi Sistemleri Denetimi Üzerine Bağımsız Denetçilere Zorunlu Eğitim Verilmelidir.



Sonuç olarak “Bağımsız Denetçilerin Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere İlişkin Görüşlerine Ait Frekans Dağılımları” incelendiğinde ortalamanın $\bar{X}=4,02$ değerini aldığı ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Standart sapma değeri ise $SS=0,441$ olarak bulunmuş ve bu değer düşük olduğu görülmektedir. Bu iki değer birlikte incelendiğinde bağımsız denetçilere göre bilgi sistemleri denetiminin bağımsız denetime etkisinin olduğu ve bu etkinin yüksek seviyede olduğu söylenebilir.

3.7.3. Bağımsız Denetçilerin e- Belge Özel Entegratör Bilgi Sistem Denetimi ile İlgili İfadelere İlişkin Bilgi Düzeyinin Analizi

Tablo 3.4’de bağımsız denetçilerin uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporuna ilişkin görüşleri ile ilgili 4 adet ifade yer almaktadır. Tabloda

katılımcılar tarafından verilen cevapların frekansı, yüzdesi, standart sapması ve ortalamaları verilmektedir.

Tablo 3.4: Bağımsız Denetçilerin Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili Görüşlerine İlişkin Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)					Veri Sayısı (n) - (%)	Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz.								
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum			
1. Uluslararası standartlara ilişkin güncel sertifikasyonlara sahip olmak bilgi sistemleri kalitesini etkiler.	2	2	13	79	24	120	4,06	0,792
2. Sızma testlerinin güncellenmesi, saldırı yöntemlerine göre test edilmesi bilgi güvenliğini etkiler.	1,7	1,7	10,8	65,8	20,	100	4,25	0,625
3 *. Sızma testlerinin kalitesi ya da sayısı bilgi sistemleri kalitesini etkilemez.	0	3	3	75	39	120	4,14	0,853
4. GİB tarafından saklama hizmeti verme izni almış firmanın, mükellefin e- Belge uygulamaları kapsamında oluşturulan belgelerinin BİS raporuna uygun olarak saklanmasını sağlaması bilgi sistemleri kalitesini artırır.	0	2	10	69	39	120	4,21	0,660
	0	1,7	8,3	57,5	32,5	100		
Ölçeğin Ortalaması ve Standart Sapması							4,16	0,466

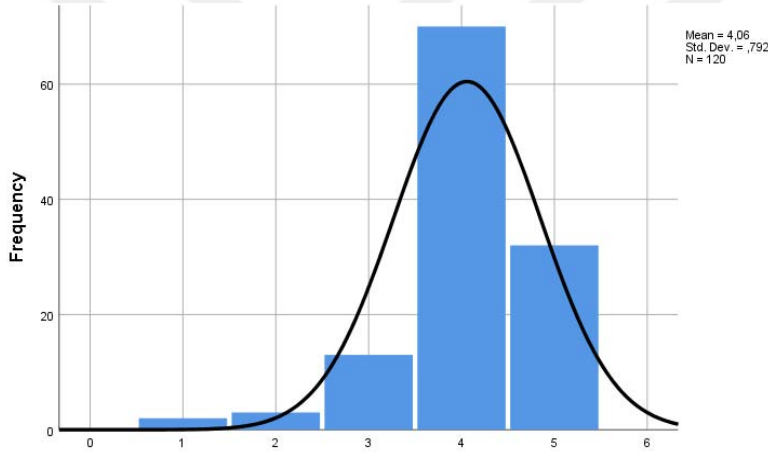
Tablo 3.4 incelendiğinde bağımsız denetçilerin uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporuna ilişkin sorulara verilen yanıtlar (1- Kesinlikle

* Bağımsız Denetçilerin Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporuna İlişkin Görüşleri boyutuna ait ifadelerden 4* bir ters ifadedir. Ters ifadeler analize alınırken SPSS programı üzerinde "Recode into Same Variables" komutu kullanılarak yeniden kodlanmıştır.

Katılmıyorum ve 5-Kesinlikle Katılıyorum aralığında) analiz edilmiş ve sonuçlara ulaşılmıştır:

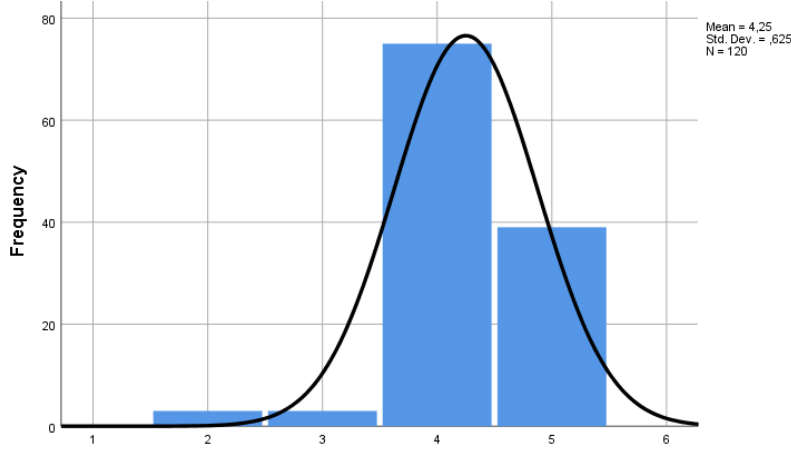
Araştırmaya katılan bağımsız denetçilerin “Uluslararası standartlara ilişkin güncel sertifikasyonlara sahip olmak bilgi sistemleri kalitesini etkiler.” ifadesine %20’si kesinlikle katıldığını, %65,8’i ise katıldığını belirtmiştir. İfadenin genel ortalamasına bakıldığında ($\bar{X}=4,06$) ortalamasına sahip olduğu ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Buna göre, katılımcıların büyük bir kısmının (%85,8) uluslararası standartlara ilişkin güncel sertifikasyonlara sahip olmanın bilgi sistemleri kalitesini etkilediğini düşünmektedirler.

Şekil 3.18: Uluslararası standartlara ilişkin güncel sertifikasyonlara sahip olmak bilgi sistemleri kalitesini etkiler.



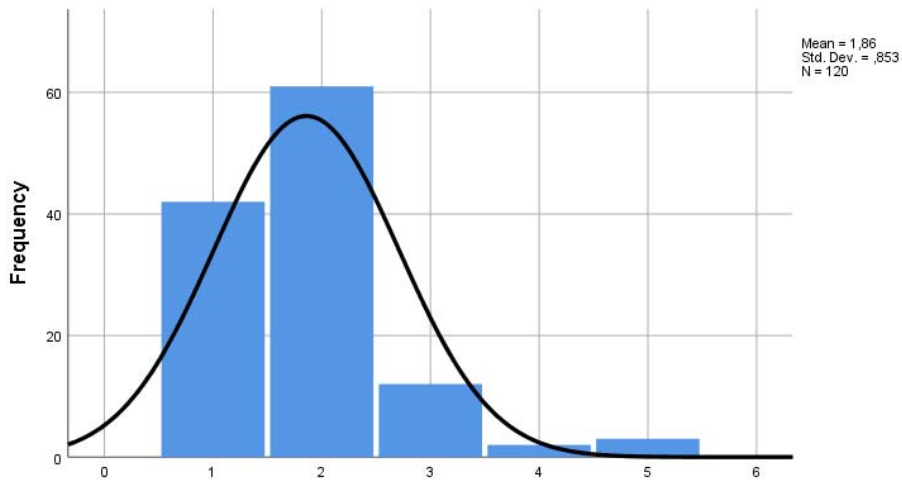
“Sızma testlerinin güncellenmesi, saldırı yöntemlerine göre test edilmesi bilgi güvenliğini etkiler.” ifadesine katılımcıların %95’i katılmış (%62,5 =katılıyorum, %32,5= kesinlikle katılıyorum), %2,5’i kararsız kalmış, %2,5’i ise katılmamıştır. İfadenin ortalamasına bakıldığında ($\bar{X}=4,25$) en yüksek değer aralığında olduğu belirlenmiş ve bu ifadenin “kesinlikle katılıyorum” değeri aralığında olduğu belirlenmiştir. Buna göre, sızma testlerinin güncellenmesinin, saldırı yöntemlerine göre test edilmesinin bilgi güvenliğini etkilediği fikri katılımcılar tarafından yüksek oranda kabul görmektedir.

Şekil 3.19: Sızma testlerinin güncellenmesi, saldırı yöntemlerine göre test edilmesi bilgi güvenliğini etkiler.



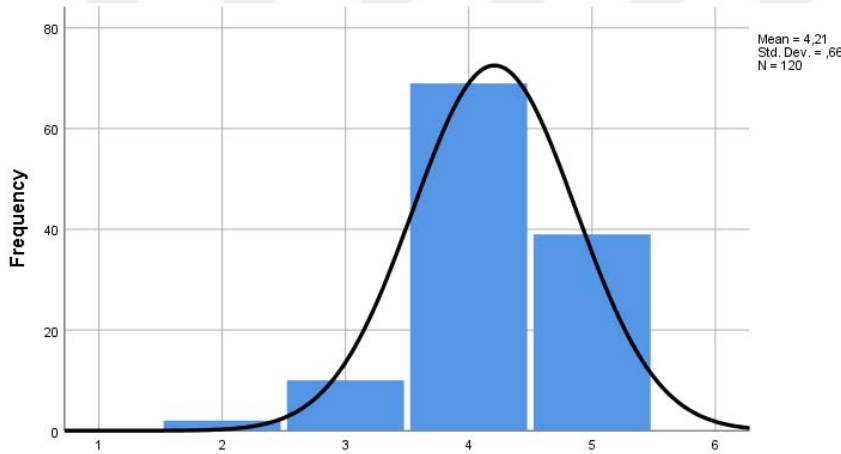
Katılımcılara sızma testi hizmeti ile ilgili ters bir formatta “Sızma testlerinin kalitesi ya da sayısı bilgi sistemleri kalitesini etkilemez.” ifadesi sunulmuştur. Katılımcıların %85’inden fazlası bu ifadeye katılmadıklarını yani sızma testlerinin kalitesi ya da sayısı bilgi sistemleri kalitesini etkiler fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=4,14$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifade standart sapma açısından bağımsız denetçilerin uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporuna ilişkin görüşleri boyutunun en yüksek değerine ($SS=0,853$) sahip olduğu da görülmektedir. Buna göre, bağımsız denetçiler, sızma testlerinin kalitesi ya da sayısının bilgi sistemleri kalitesini etkilediğini belirtmektedirler.

Şekil 3.20: Sızma testlerinin kalitesi ya da sayısı bilgi sistemleri kalitesini etkilemez.



Araştırmaya katılan katılımcıların “GİB tarafından saklama hizmeti verme izni almış firmanın, mükellefin e-Belge uygulamaları kapsamında oluşturulan belgelerinin BİS raporuna uygun olarak saklanması sağlanması bilgi sistemleri kalitesini artırır.” ifadesine verdikleri cevaplar %32,5 kesinlikle katılıyorum ve %57,5 katılıyorum şeklindedir. İfadenin ortalamasına bakıldığında ($\bar{X}=4,21$ “kesinlikle katılıyorum”) yüksek bir değer aralığında olduğu belirlenmiştir. Buna göre katılımcıların büyük bir çoğunluğu GİB tarafından saklama hizmeti verme izni almış firmanın, mükellefin e-Belge uygulamaları kapsamında oluşturulan belgelerinin BİS raporuna uygun olarak saklanması sağlanması bilgi sistemleri kalitesini artırır fikrine katılmaktadır.

Şekil 3.21: GİB tarafından saklama hizmeti verme izni almış firmanın, mükellefin e-Belge uygulamaları kapsamında oluşturulan belgelerinin BİS raporuna uygun olarak saklanması sağlanması bilgi sistemleri kalitesini artırır.



Sonuç olarak bağımsız denetçilerin uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporuna etkisine dair görüşleri ile ilgili ifadelerin ortalamasının $\bar{X}=4,16$ ve standart sapmasının $SS=0,466$ değerinde olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporuna ait ifadelerle katılma ölçeğinin yüksek seviyede olduğu söylenebilir.

Aşağıda yer alan Tablo 3.5’ de iç kontrol ve denetim mekanizmalarına ilişkin ifadeler ile ilgili 4 ifade bulunmakta ve katılımcılar tarafından bu ifadelerle verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.5: Bağımsız Denetçilerin İç Kontrol ve Denetim Mekanizmalarına İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

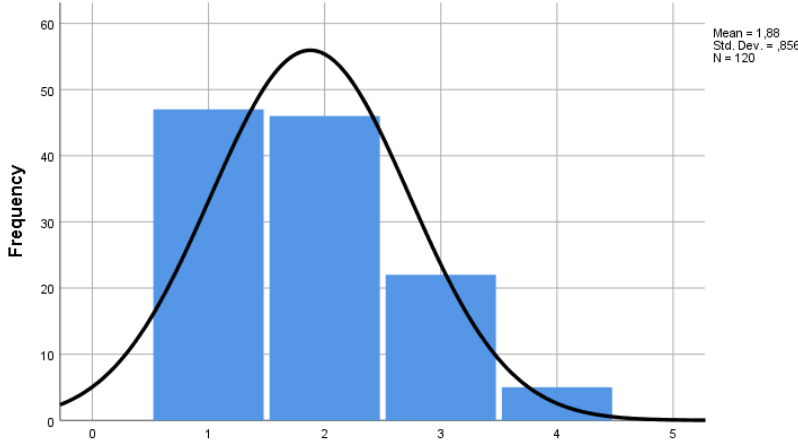
Ölçek Maddeleri	Frekans (f)						Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum	Veri Sayısı (n) - (%)		
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1*. İç kontrol ve iç denetim dokümanı oluşturulması bilgi sistemleri kalitesini etkilemez.	0	5	22	46	47	120	4,13	0,856
2. İç kontrol dokümanları ile iş sürekliliği belgelerinin birbiriyle uyumlu olması bilgi sistemleri kalitesini etkiler.	0	4,2	18,3	38,3	39,2	100	4,22	0,582
3*. İç kontrol denetimlerinin periyodik biçimde yapılması ve denetim sonuçlarının raporlanması bilgi sistemleri kalitesini etkilemez.	2	11	14	56	37	120	3,96	0,974
	1,7	9,2	11,7	46,7	30,8	100		
Ölçeğin Ortalaması ve Standart Sapması							4,10	0,643

Yukarıdaki tabloda yer alan ifadelere katılımcıların verdikleri yanıtlar analiz edilmiş ve aşağıdaki sonuçlara ulaşılmıştır.

Katılımcılara ters bir formatta; “İç kontrol ve iç denetim dokümanı oluşturulması bilgi sistemleri kalitesini etkilemez.” ifadesi sunulmuştur. Katılımcıların %77,5’inden fazlası bu ifadeye katılmadıklarını yani iç kontrol ve iç denetim dokümanı oluşturulması bilgi sistemleri kalitesini etkiler fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=4,13$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır.

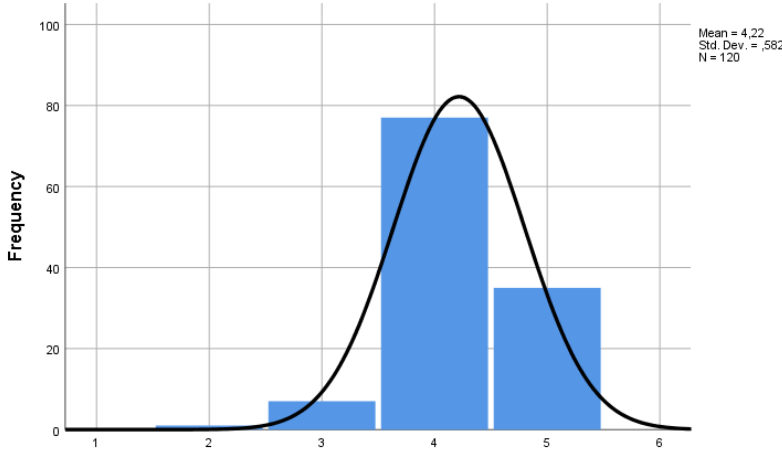
* İç Kontrol ve Denetim Mekanizmalarına İlişkin ifadelerinden 1* ve 3* ters ifadelerdir. Ters ifadeler analize alınırken SPSS programı üzerinde “Recode into Same Variables” komutu kullanılarak yeniden kodlanmıştır.

Şekil 3.22: İç kontrol ve iç denetim dokümanı oluşturulması bilgi sistemleri kalitesini etkilemez.



Araştırmaya katılan katılımcıların büyük bir kısmı (%93,4) “İç kontrol dokümanları ile iş sürekliliği belgelerinin birbiriyle uyumlu olması bilgi sistemleri kalitesini etkiler.” ifadesine katıldığı (%64,2=katılıyorum, %29,2=kesinlikle katılıyorum), %5,8’inin kararsız kaldığı görülmektedir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,22$) iç kontrol ve denetim mekanizmalarına ilişkin boyutunun en yüksek ortalamasına sahip olduğu ve ifadenin “kesinlikle katılıyorum” değeri aralığında olduğu görülmektedir.

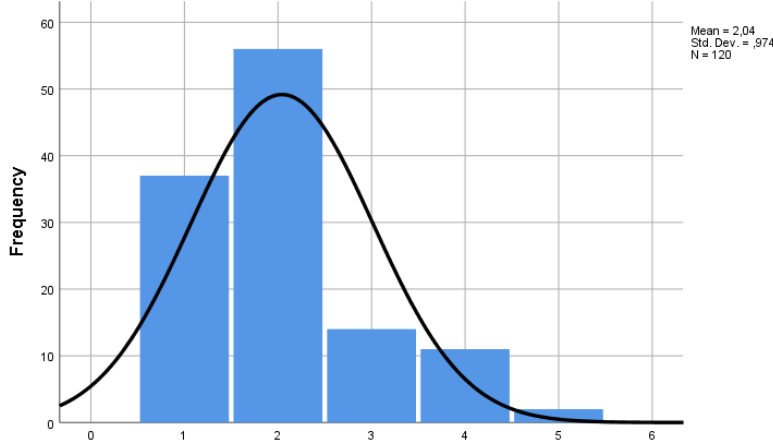
Şekil 3.23: İç Kontrol Dökümanları ile İş Sürekliliği Belgelerinin Birbiriyle Uyumlu Olması Bilgi Sistemleri Kalitesini Etkiler.



Katılımcılara iç kontrol ve denetim mekanizmalarına ilişkin ters bir formatta “İç kontrol denetimlerinin periyodik biçimde yapılması ve denetim sonuçlarının raporlanması bilgi sistemleri kalitesini etkilemez.” ifadesi sunulmuştur. Katılımcıların %76,8’i bu ifadeye katıldığı (%46,7=katılıyorum, %30,8=kesinlikle katılıyorum), %11,7’sinin kararsız kaldığı ve geriye kalan %10,9’unun ise katılmadığı görülmektedir.

Bu ifadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,96$ “katılıyorum”) yüksek bir değer aralığında olduğu belirlenmiştir.

Şekil 3.24: İç kontrol denetimlerinin periyodik biçimde yapılması ve denetim sonuçlarının raporlanması bilgi sistemleri kalitesini etkilemez.



Sonuç olarak bağımsız denetçilerin iç kontrol ve denetim mekanizmalarına ilişkin ifadelerle ilgili ortalamasının $\bar{X}=4,10$ ve standart sapmasının $SS=0,643$ değerinde olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin iç kontrol ve denetim mekanizmalarına ilişkin ifadelerle ilgili katılım ölçeğinin yüksek seviyede olduğu söylenebilir.

Aşağıda yer alan Tablo 3.6’ da personelin niteliğine ilişkin 4 ifade bulunmakta ve katılımcılar tarafından bu ifadelerle verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.6: Bağımsız Denetçilerin Personelin Niteliğine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)					Veri Sayısı (n) - (%)	Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz.								
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum			
1*. İstihdam edilen personelin öğrenimi ve sertifikasyonlarının göreviyle uygun olması bilgi sistemleri kalitesini etkilemez.	0	6	17	54	43	120	4,12	0,832
2. Sistemlerin yönetiminde, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görev ve sorumlulukların ayrılığı prensibinin uygulanması bilgi sistemleri kalitesini artırır.	0	0	7	72	41	120	4,28	0,568
3*. Uygun nitelik ve sayıda personel istihdamı bilgi sistemleri kalitesini artırmaz.	1	6	18	59	36	120	4,03	0,855
4. Özel Entegratör yönetici ve çalışanlarının kamusal bir görev ifa ettiklerinin bilinci ile hareket etmeleri bilgi sistemleri kalitesini artırır.	0	0	11	61	48	120	4,31	0,632
Ölçeğin Ortalaması ve Standart Sapması							4,15	0,594

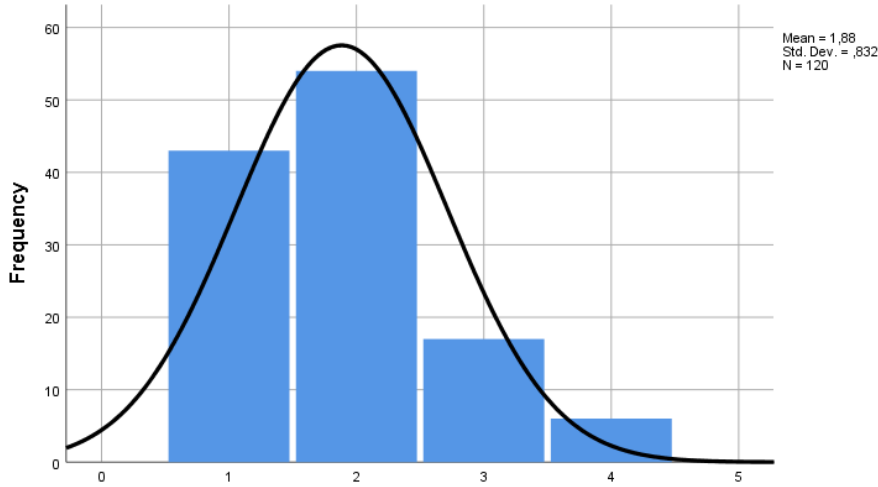
Tablo 3.6'da görüldüğü üzere personelin niteliğine ilişkin ifadelerle ilgili katılımcıların (1- Kesinlikle Katılmıyorum ve 5-Kesinlikle Katılıyorum aralığında) verdikleri yanıtlar analiz edilmiş ve sonuçlara ulaşılmıştır:

Katılımcılara personelin niteliğine ilişkin ters bir formatta “İstihdam edilen personelin öğrenimi ve sertifikasyonlarının göreviyle uygun olması bilgi sistemleri kalitesini etkilemez.” ifadesi sunulmuştur. Katılımcıların %80,8'i bu ifadeye katılmadıklarını yani personelin öğrenimi ve sertifikasyonlarının göreviyle uygun

* Personel Niteliği ifadelerinden 1* ve 3* ters ifadelerdir. Ters ifadeler analize alınırken SPSS programı üzerinde “Recode into Same Variables” komutu kullanılarak yeniden kodlanmıştır.

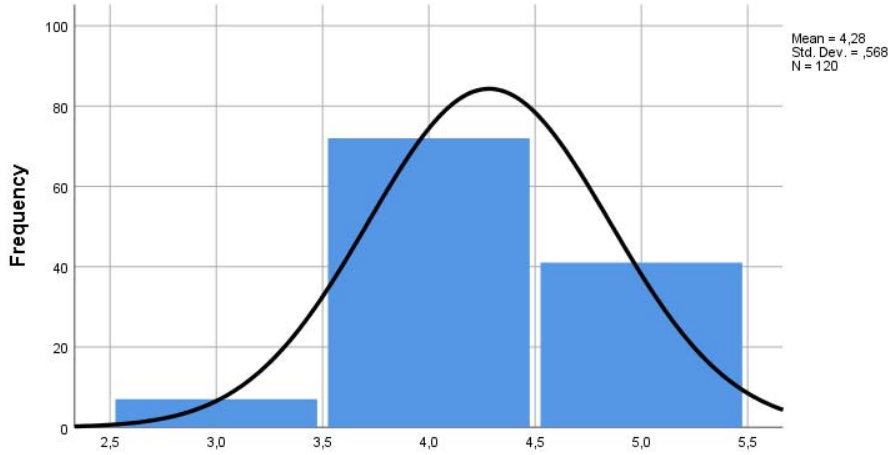
olmasının bilgi sistemleri kalitesini etkileyeceğini belirtmişlerdir. Diğer taraftan katılımcıların %5'i bu fikre katıldıklarını ve %14,2'si kararsız kaldıklarını belirtmişlerdir. Bu ifadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=4,12$ “katılıyorum”) yüksek bir değer aralığında olduğu görülür. Bu bağlamda, istihdam edilen personelin öğrenimi ve sertifikasyonlarının göreviyle uygun olmasının bilgi sistemleri kalitesini olumlu yönde etkileyeceği bağımsız denetçiler tarafından düşünülmektedir.

Şekil 3.25: İstihdam edilen personelin öğrenimi ve sertifikasyonlarının göreviyle uygun olması bilgi sistemleri kalitesini etkilemez.



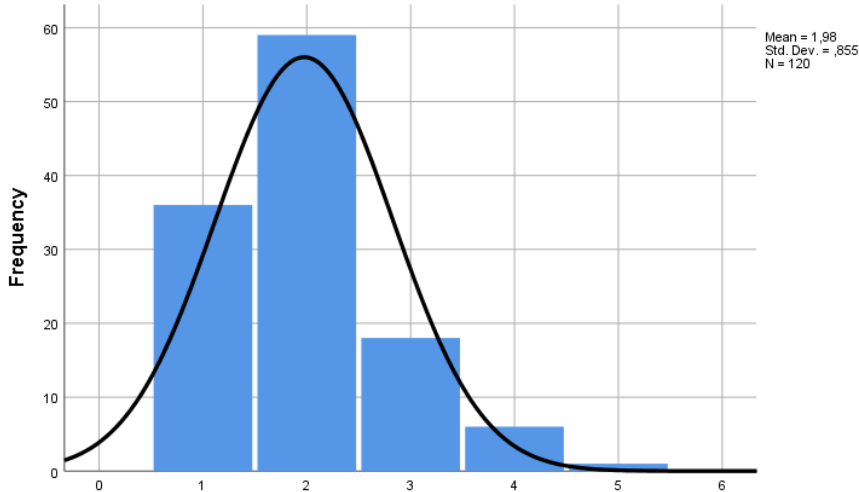
“Sistemlerin yönetiminde, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görev ve sorumlulukların ayrılığı prensibinin uygulanması bilgi sistemleri kalitesini artırır.” ifadesi katılımcılara sunulmuştur. Katılımcıların büyük bir çoğunluğu (%94,2) bu ifadeye katıldıklarını (%60=katılıyorum, %34,2=kesinlikle katılıyorum) ve geriye kalan %5,8'i kararsız kaldıklarını belirtmişlerdir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,28$ “ kesinlikle katılıyorum”) yüksek bir değer aralığında olduğu görülür. Ayrıca bu ifadenin standart sapma açısından personelin niteliğine ilişkin boyutunun en düşük değerine ($SS=0,568$) sahip olduğu görülmektedir. Bu veriler doğrultusunda, katılımcıların büyük bir çoğunluğu görev ve sorumlulukların ayrılığı prensibinin bilgi sistemleri kalitesini artıracığını belirtmektedirler.

Şekil 3.26: Sistemlerin yönetiminde, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görev ve sorumlulukların ayrılığı prensibinin uygulanması bilgi sistemleri kalitesini artırır.



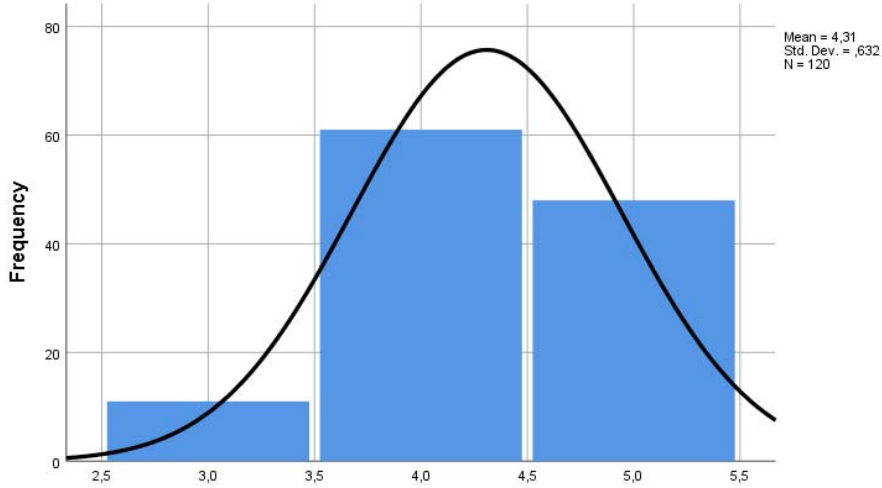
Katılımcılara personelin niteliğine ilişkin ters bir formatta “Uygun nitelik ve sayıda personel istihdamı bilgi sistemleri kalitesini artırır.” ifadesi sunulmuştur. Katılımcıların %79,2’si bu ifadeye katılmadıklarını yani uygun nitelik ve sayıda personel istihdamının bilgi sistemleri kalitesini artırır olarak görüşlerini belirtmişlerdir. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=4,03$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifade standart sapma açısından personel niteliği boyutunun en yüksek değerine ($SS=0,855$) sahip olduğu da görülmektedir. Buna göre, uygun nitelik ve sayıda personelin istihdamının bilgi sistemleri kalitesini artırdığını düşünen bağımsız denetçiler çoğunlukta olsa da tam tersini savunan (%20’lik) tarafın da azımsanmayacak bir çoğunluğa sahip olduğu görülmektedir.

Şekil 3.27: Uygun nitelik ve sayıda personel istihdamı bilgi sistemleri kalitesini artırır.



Katılımcılar, personel niteliği ile ilgili “Özel Entegratör yönetici ve çalışanlarının kamusal bir görev ifa ettiklerinin bilinci ile hareket etmeleri bilgi sistemleri kalitesini artırır.” ifadesine verdikleri yanıt kesinlikle katılıyorum (%40) ve katılıyorum (%50,8) şeklindedir. Bu yüksek katılımı (%90,8) ifadenin ortalamasına bakıldığında ($\bar{X}=4,31$) katılımcıların çoğu bu ifadeye “kesinlikle katılıyorum” dediği anlaşılmaktadır. Buna göre, katılımcıların; Özel entegratör yönetici ve çalışanlarının kamusal bir görev ifa ettiklerinin bilinci ile hareket etmelerinin bilgi sistemleri kalitesini artırdığına yönelik bir algıya sahip olduğu söylenebilir.

Şekil 3.28: Özel Entegratör yönetici ve çalışanlarının kamusal bir görev ifa ettiklerinin bilinci ile hareket etmeleri bilgi sistemleri kalitesini artırır.



Sonuç olarak bağımsız denetçilerin personel niteliğine ilişkin ifadelerle ait görüşlerinin ortalamasının $\bar{X}=4,15$ ve standart sapmasının $SS=0,594$ değerinde olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin personel niteliğine ilişkin ifadelerle katılma ölçeğinin yüksek seviyede olduğu söylenebilir.

Tablo 3.7’ de fiziki şartlar ve güvenlik tedbirlerine ilişkin 3 ifade bulunmakta ve katılımcılar tarafından bu ifadelerle verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.7: Bağımsız Denetçilerin Fiziki Şartlar ve Güvenlik Tedbirlerine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)					Veri Sayısı (n) - (%)	Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum			
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1. Hassas verilerin (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanıyor olması bilgi sistemleri kalitesini artırır.	1	9	7	65	38	120	4,08	0,866
2. Veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin durmasına izin verecek bir yapılanma olmadığının kontrol edilmesi bilgi sistemleri kalitesini artırır.	5	6	19	55	35	120	3,91	1,012
3*. Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gerekliliklerinin sağlanması bilgi sistemleri kalitesini artırmaz.	4	11	18	53	34	120	3,85	1,042
Ölçeğin Ortalaması ve Standart Sapması							3,94	0,658

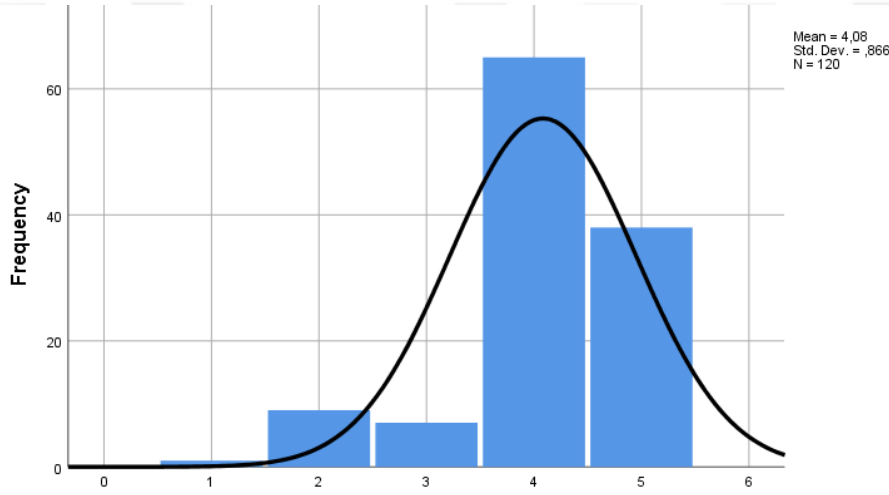
Tablo 3.7’de görüldüğü üzere fiziki şartlar ve güvenlik tedbirlerine ilişkin ifadelerle ilgili katılımcıların (1- Kesinlikle Katılmıyorum ve 5-Kesinlikle Katılıyorum aralığında) verdikleri yanıtlar analiz edilmiş ve sonuçlara ulaşılmıştır.

“Hassas verilerin (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanıyor olması bilgi sistemleri kalitesini artırır.” ifadesi katılımcılara sunulmuş olup

* Fiziki Şartlar ve Güvenlik Tedbirleri ifadelerinden 3* ters ifadelerdir. Ters ifadeler analize alınırken SPSS Programı üzerinde “Recode into Same Variables” komutu kullanılarak yeniden kodlanmıştır.

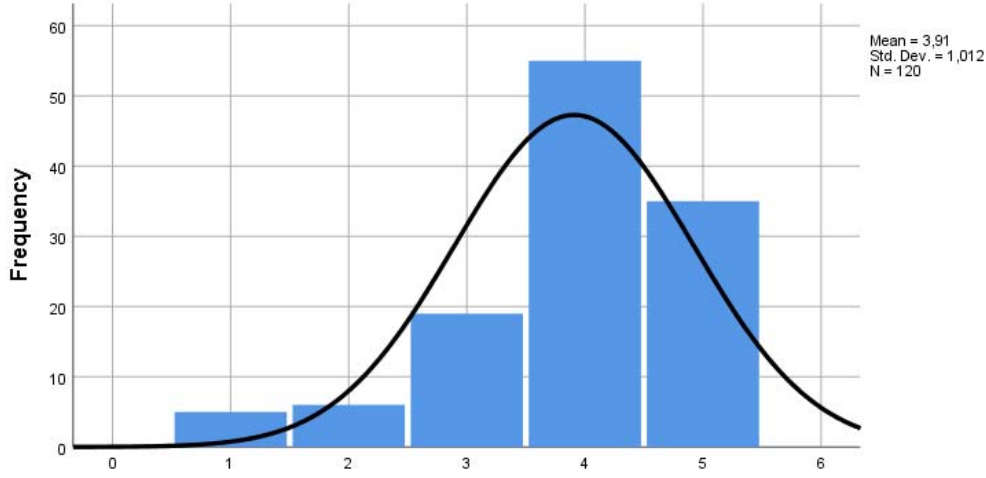
katılımcıların büyük bir çoğunluğu (%85,7) bu ifadeye katıldıklarını (%54,2=katılıyorum, %31,7=kesinlikle katılıyorum), %5,8'i kararsız kaldıklarını ve %8,3'ü katılmadıklarını belirtmişlerdir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,08$ “katılıyorum”) yüksek bir değer aralığında olduğu görülür. Ayrıca bu ifadenin standart sapma açısından fiziki şartlar ve güvenlik tedbirlerine ilişkin en düşük değerine ($SS=0,866$) sahip olduğu görülmektedir. Bu veriler doğrultusunda, katılımcıların büyük bir çoğunluğu hassas verilerin (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanması olmasının bilgi sistemleri kalitesini artıracaklarını belirtmektedirler.

Şekil 3.29: Hassas verilerin (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanması bilgi sistemleri kalitesini artırır.



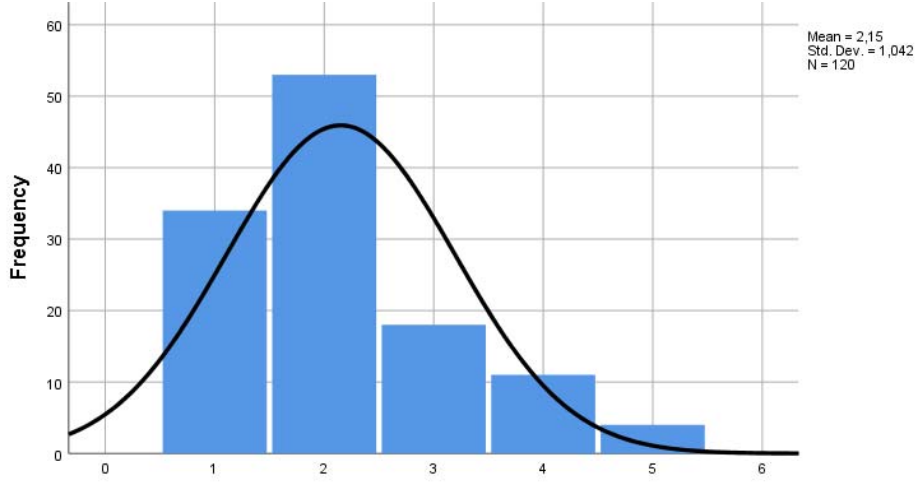
Katılımcılar, fiziki şartlar ve güvenlik tedbirleri ile ilgili “Veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin durmasına izin verecek bir yapılanma olmadığı kontrol edilmesi bilgi sistemleri kalitesini artırır.” ifadesine verdikleri yanıt kesinlikle katılıyorum (%29,2) ve katılıyorum (%45,8) şeklindedir. Bu katılımla (%75) ifadenin ortalamasına bakıldığında ($\bar{X} = 3,91$) katılımcıların çoğu bu ifadeye “katılıyorum” dediği anlaşılmaktadır. Buna göre, katılımcıların; veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin durmasına izin verecek bir yapılanma olmadığı kontrol edilmesinin bilgi sistemleri kalitesini artırdığına yönelik bir algıya sahip olduğu söylenebilir.

Şekil 3.30: Veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin durmasına izin verecek bir yapılanma olmadığının kontrol edilmesi bilgi sistemleri kalitesini artırır.



Katılımcılara, ters bir formatta “Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gerekliliklerinin sağlanması bilgi sistemleri kalitesini artırır.” ifadesi sunulmuştur. Katılımcıların %72,5’i bu ifadeye katılmadıklarını yani sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gerekliliklerinin sağlanması bilgi sistemleri kalitesini artırır fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,85$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifade standart sapma açısından fiziki şartlar ve güvenlik tedbirlerine ilişkin en yüksek değerine ($SS=1,042$) sahip olduğu da görülmektedir. Buna göre, sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gerekliliklerinin sağlanmasının bilgi sistemleri kalitesini artırdığını düşünen bağımsız denetçiler çoğunlukta olsa da tam tersini savunan (%12,2’lik) tarafın da azımsanmayacak bir çoğunluğa sahip olduğu görülmektedir.

Şekil 3.31: Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gerekliliklerinin sağlanması bilgi sistemleri kalitesini artırmaz.



Sonuç olarak bağımsız denetçilerin fiziki şartlar ve güvenlik tedbirlerine ilişkin ifadelerine dair görüşlerinin ortalamasının $\bar{X}=3,94$ ve standart sapmasının $SS=0,658$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin fiziki şartlar ve güvenlik tedbirleri ile ilgili fikirlerinin yüksek seviyede olduğu söylenebilir.

Aşağıda yer alan Tablo 3.8’de erişim güvenliğine ilişkin 3 ifade bulunmakta ve katılımcılar tarafından bu ifadelerine verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.8: Bağımsız Denetçilerin Erişim Güvenliğine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)						Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum	Veri Sayısı (n) - (%)		
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz. 1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1*. Hassas verilere herhangi bir personelin tek başına erişim yetkisinin olmaması bilgi sistemleri kalitesini artırmaz.	5	15	23	48	29	120	3,68	1,101
2. Sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtların güvenli biçimde tutuluyor olması bilgi sistemleri kalitesini artırır.	2	1	7	68	42	120	4,22	0,739
3*. Tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş olması bilgi sistemleri kalitesini artırmaz.	3	10	24	52	31	120	3,82	0,996
Ölçeğin Ortalaması ve Standart Sapması							3.09	0,639

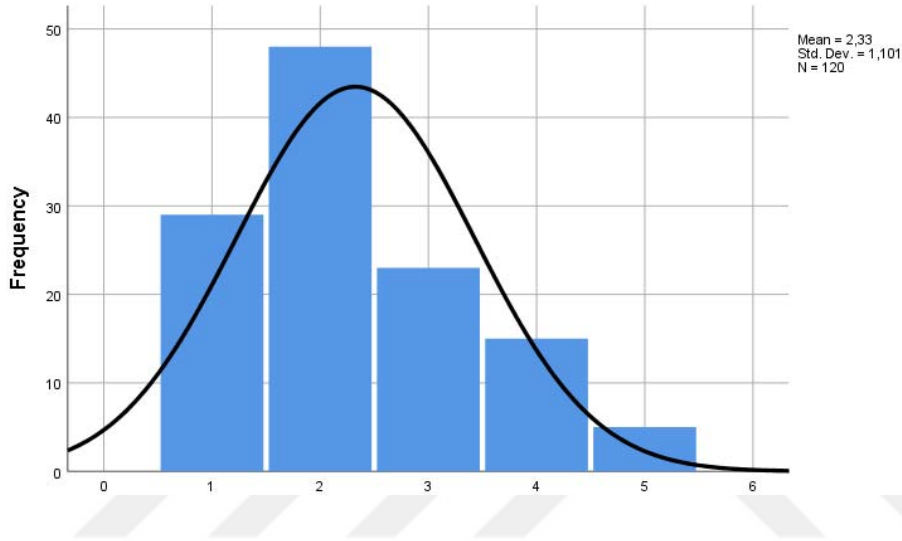
Yukarıdaki tabloda yer alan ifadelere katılımcıların (1- Kesinlikle Katılmıyorum ve 5-Kesinlikle Katılıyorum) aralığında verdikleri yanıtlar analiz edilmiş ve aşağıdaki sonuçlara ulaşılmıştır.

Katılımcılara erişim güvenliğine ilişkin ters bir formatta “Hassas verilere herhangi bir personelin tek başına erişim yetkisinin olmaması bilgi sistemleri kalitesini artırmaz.” ifadesi sunulmuştur. Katılımcıların %64,2’si bu ifadeye katılmadıklarını yani hassas verilere herhangi bir personelin tek başına erişim yetkisinin olmamasının bilgi sistemleri kalitesini artıracığı fikrini belirtmişlerdir. Diğer taraftan katılımcıların %12,5’i bu fikre

** Erişim Güvenliği ifadelerinden 1* ve 3* ters ifadelerdir. Ters ifadeler analize alınırken SPSS programı üzerinde “Recode into Same Variables” komutu kullanılarak yeniden kodlanmıştır.

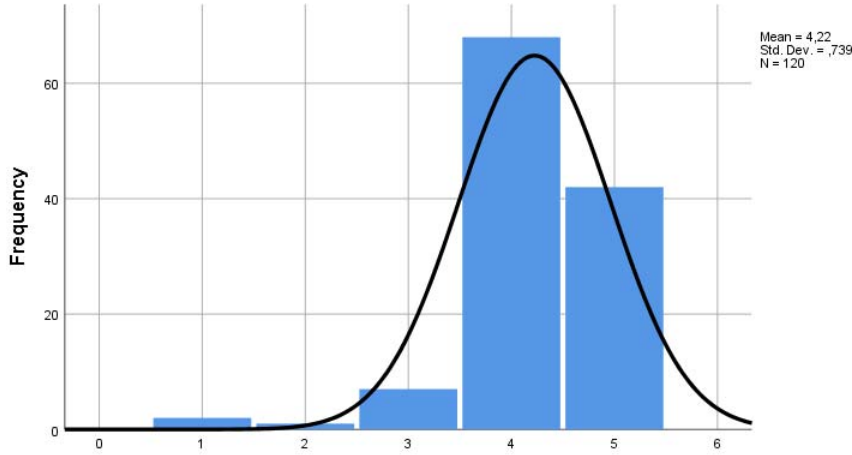
katıldıklarını ve %19,2'si kararsız kaldıklarını belirtmişlerdir. Bu ifadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,68$ “katılıyorum”) yüksek bir değer aralığında olduğu görülür. Bu bağlamda, hassas verilere herhangi bir personelin tek başına erişim yetkisinin olmaması bilgi sistemleri kalitesini olumlu yönde etkileyeceği bağımsız denetçiler tarafından düşünülmektedir.

Şekil 3.32: Hassas verilere herhangi bir personelin tek başına erişim yetkisinin olmaması bilgi sistemleri kalitesini artırmaz.



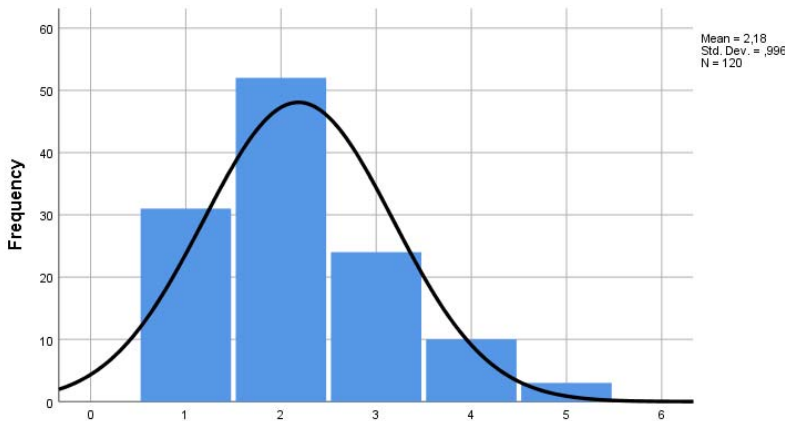
“Sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtların güvenli biçimde tutuluyor olması bilgi sistemleri kalitesini artırır.” İfadesi katılımcılara sorulmuştur. Katılımcıların büyük bir çoğunluğu (%91,7) bu ifadeye katıldıklarını (%56,7=katılıyorum, %35=kesinlikle katılıyorum) ve %5,8'i kararsız kaldıklarını belirtmişlerdir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,22$ “kesinlikle katılıyorum”) yüksek bir değer aralığında olduğu görülür. Ayrıca bu ifadenin standart sapma açısından erişim güvenliğine ilişkin boyutunun en düşük değerine ($SS=0,739$) sahip olduğu görülmektedir. Bu veriler doğrultusunda, katılımcıların büyük bir çoğunluğu sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtların güvenli biçimde tutuluyor olmasının bilgi sistemleri kalitesini artıracığını belirtmektedirler.

Şekil 3.33: Sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtların güvenli biçimde tutuluyor olması bilgi sistemleri kalitesini artırır



Katılımcılara ters bir formatta “Tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş olması bilgi sistemleri kalitesini artırmaz” ifadesi sunulmuştur. Katılımcıların %68,8’i bu ifadeye katılmadıklarını yani tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş olmasının bilgi sistemleri kalitesini artırır fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,82$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifadenin standart sapma değeri (SS=0,996) olarak hesaplanmıştır. Buna göre, tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş olması bilgi sistemleri kalitesini artırır düşüncesine sahip olan bağımsız denetçiler çoğunlukta olsa da kararsız olan (%20’lik) tarafın da azımsanmayacak bir kısma sahip olduğu görülmektedir.

Şekil 3.34: Tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş olması bilgi sistemleri kalitesini artırmaz.



Sonuç olarak bağımsız denetçilerin erişim güvenliğine ilişkin ifadelerle dair görüşlerinin ortalamasının $\bar{X}=3,09$ ve standart sapmasının $SS=0,639$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “kararsızım” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin erişim güvenliği ile ilgili fikirlerinin orta seviyede olduğu söylenebilir. Tablo 3.9 'da iş sürekliliği, risk yönetimi ve acil durum planlarına ilişkin 3 ifade bulunmakta ve yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.9: Bağımsız Denetçilerin İş Sürekliliği, Risk Yönetimi ve Acil Durum Planlarına İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

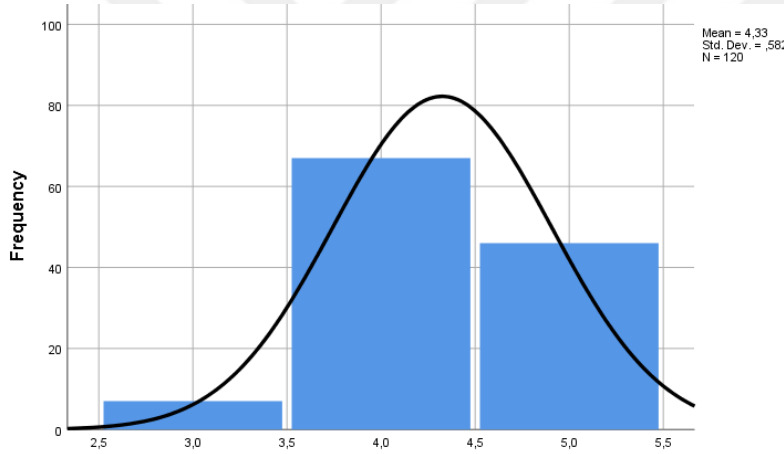
Ölçek Maddeleri	Frekans (f)					Veri Sayısı (n) - (%)	Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum			
Aşağıda yer alan ifadelerle katılma düzeyinizi lütfen belirtiniz.								
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1. Özel entegratörün, bir risk yönetim planı oluşturması bilgi sistemleri kalitesini artırır.	0	0	7	67	46	120	4,33	0,582
2*. Donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olayların risk yönetim planına dâhil edilmesi bilgi sistemleri kalitesini artırmaz.	2	11	13	55	39	120	3,91	1,061
3*. Bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet veremez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanması bilgi sistemleri kalitesini artırmaz.	2	11	13	55	39	120	3,98	0,979
Ölçeğin Ortalaması ve Standart Sapması							4,07	0,703

* İş Sürekliliği, Risk Yönetimi ve Acil Durum Planlarına ilişkin ifadelerden 2* ve 3* ters ifadelerdir. Ters ifadeler analize alınırken SPSS programı üzerinde “Recode into Same Variables” komutu kullanılarak yeniden kodlanmıştır.

Tablo 3.9’da görüldüğü üzere iş sürekliliği, risk yönetimi ve acil durum planlarına ilişkin ifadelerle ilgili katılımcıların (1-Kesinlikle Katılmıyorum ve 5-Kesinlikle Katılıyorum aralığında) verdikleri yanıtlar analiz edilmiş ve sonuçlara ulaşılmıştır.

Katılımcılar, iş sürekliliği, risk yönetimi ve acil durum planlarına ilişkin “Özel entegratörün, bir risk yönetim planı oluşturması bilgi sistemleri kalitesini artırır.” ifadesine verdikleri yanıt kesinlikle katılıyorum (%38,3) ve katılıyorum (%55,8) şeklindedir. Bu yüksek katılımı (%94,1) ifadenin ortalamasına bakıldığında ($\bar{X}=4,33$) katılımcıların çoğu bu ifadeye “kesinlikle katılıyorum” dediği anlaşılmaktadır. Buna göre, katılımcıların; Özel entegratörün, bir risk yönetim planı oluşturmasının bilgi sistemleri kalitesini artırdığına yönelik bir algıya sahip olduğu söylenebilir.

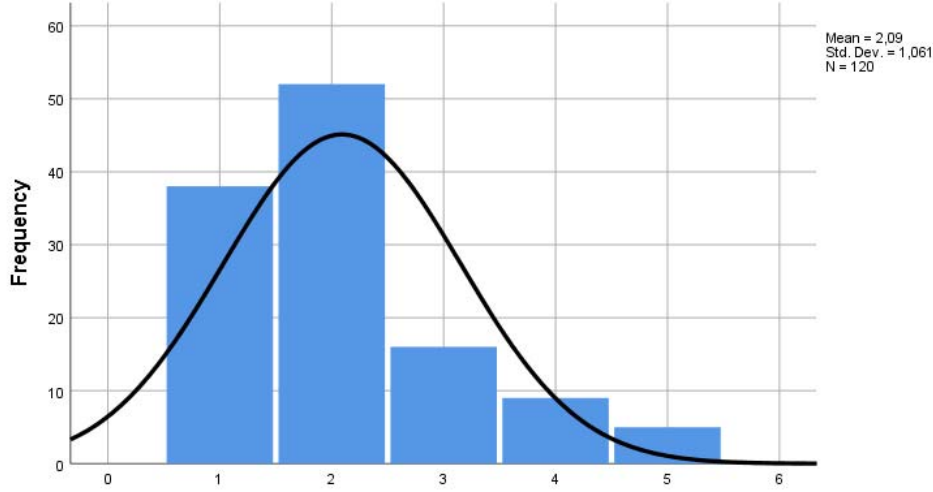
Şekil 3.35: Özel entegratörün, bir risk yönetim planı oluşturması bilgi sistemleri kalitesini artırır.



Katılımcılara, ters bir formatta “Donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olayların risk yönetim planına dâhil edilmesi bilgi sistemleri kalitesini artırmaz.” ifadesi sunulmuştur. Katılımcıların %78,3’ü bu ifadeye katılmadıklarını yani donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olayların risk yönetim planına dâhil edilmesinin bilgi sistemleri kalitesini artırır fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,91$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifade standart sapma açısından personel niteliği boyutunun en yüksek değerine ($SS=1,061$) sahip olduğu da görülmektedir. Buna göre, donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı

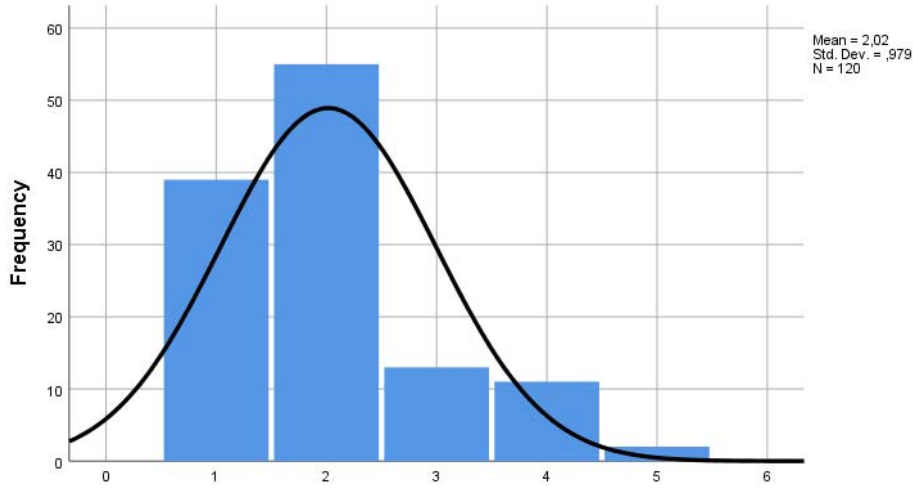
olayların risk yönetim planına dâhil edilmesinin bilgi sistemleri kalitesini artırdığını düşünen bağımsız denetçiler çoğunlukta olsa da tam tersini savunan (%10,9'luk) tarafın da olduğu görülmektedir.

Şekil 3.36: Donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olayların risk yönetim planına dâhil edilmesi bilgi sistemleri kalitesini artırmaz.



Katılımcılara, ters bir formatta “Bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet veremez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanması bilgi sistemleri kalitesini artırmaz.” ifadesi sunulmuştur. Katılımcıların %78,3’ü bu ifadeye katılmadıklarını yani bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet veremez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanmasının bilgi sistemleri kalitesini artıracığı fikrini belirtmişlerdir. Diğer taraftan katılımcıların %10,9’u bu fikre katıldıklarını ve %10,8’i kararsız kaldıklarını belirtmişlerdir. Bu ifadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,98$ “katılıyorum”) yüksek bir değer aralığında olduğu görülür. Bu bağlamda, bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet veremez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanmasının bilgi sistemleri kalitesini olumlu yönde etkileyeceği bağımsız denetçiler tarafından düşünülmektedir.

Şekil 3.37: Bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet veremez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanması bilgi sistemleri kalitesini artırmaz.



Sonuç olarak bağımsız denetçilerin iş sürekliliği, risk yönetimi ve acil durum planlarına ilişkin ifadelerle dair görüşlerinin ortalamasının $\bar{X}=3,98$ ve standart sapmasının $SS=0,979$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin iş sürekliliği, risk yönetimi ve acil durum planlarına ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.

Aşağıda yer alan Tablo 3.10’da denetim izleri yönetimine ilişkin 3 ifade bulunmakta ve katılımcılar tarafından bu ifadelerle verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.10: Bağımsız Denetçilerin Denetim İzleri Yönetimine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

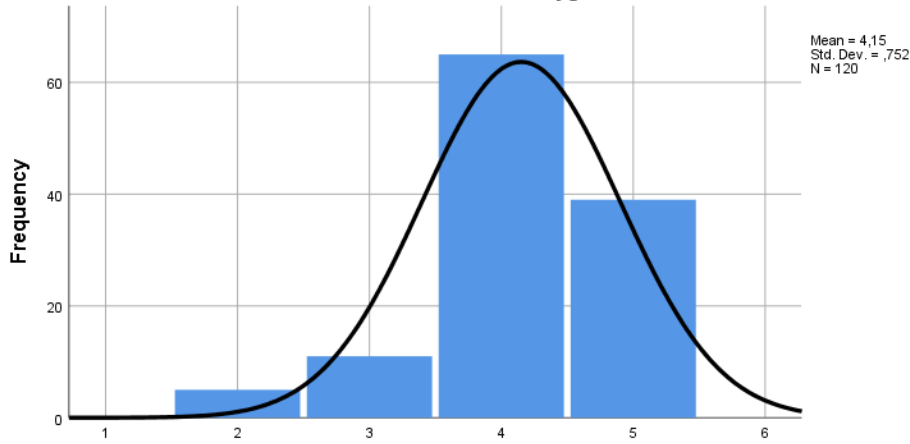
Ölçek Maddeleri	Frekans (f)					Veri Sayısı (n) - (%)	Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum			
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz. 1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1. Özel entegratörün, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef ve GİB ile haberleşmesinde kullanılan yazılım uygulamalarının veri tabanı motorları ve uygulama kayıtlarını tutması (denetim izi) bilgi sistemleri kalitesini artırır.	0	5	11	65	39	120	4,15	0,752
2*.Denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınması bilgi sistemleri kalitesini artırmaz.	0	4,2	9,2	54,2	32,5	100,0	3,83	1,015
3.Denetim İzleri yönetimi için veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl oluştuğunun ve saklandığının kayıt altına alınmış olması bilgi sistemleri kalitesini artırır.	1	1	14	55	49	120	4,25	0,759
Ölçeğin Ortalaması ve Standart Sapması	0,8	0,8	11,7	45,8	40,8	100,0	4.07	0,646

Tablo 3.10'da görüldüğü üzere denetim izleri yönetimine ilişkin ifadelerle ilgili katılımcıların (1-Kesinlikle Katılmıyorum ve 5-Kesinlikle Katılıyorum aralığında) verdikleri yanıtlar analiz edilmiş ve sonuçlara ulaşılmıştır.

* Denetim İzleri Yönetimine ilişkin ifadelerden 2* ters ifadedir. Ters ifadeler analize alınırken SPSS programı üzerinde "Recode into Same Variables" komutu kullanılarak yeniden kodlanmıştır.

“Özel entegratörün, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef ve GİB ile haberleşmesinde kullanılan yazılım uygulamalarının veri tabanı motorları ve uygulama kayıtlarını tutması (denetim izi) bilgi sistemleri kalitesini artırır.” ifadesine katılımcıların %86,7’i katılmış (%54,2 =katılıyorum, %32,5= kesinlikle katılıyorum), %9,2’si kararsız kalmış, %4,2’si ise katılmamıştır. İfadenin ortalamasına bakıldığında ($\bar{X}=4,15$) yüksek değer aralığında olduğu belirlenmiş ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Buna göre, özel entegratörün, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef ve GİB ile haberleşmesinde kullanılan yazılım uygulamalarının veri tabanı motorları ve uygulama kayıtlarını tutması (denetim izi) bilgi sistemleri kalitesini artırır fikri katılımcılar tarafından yüksek oranda kabul görmektedir.

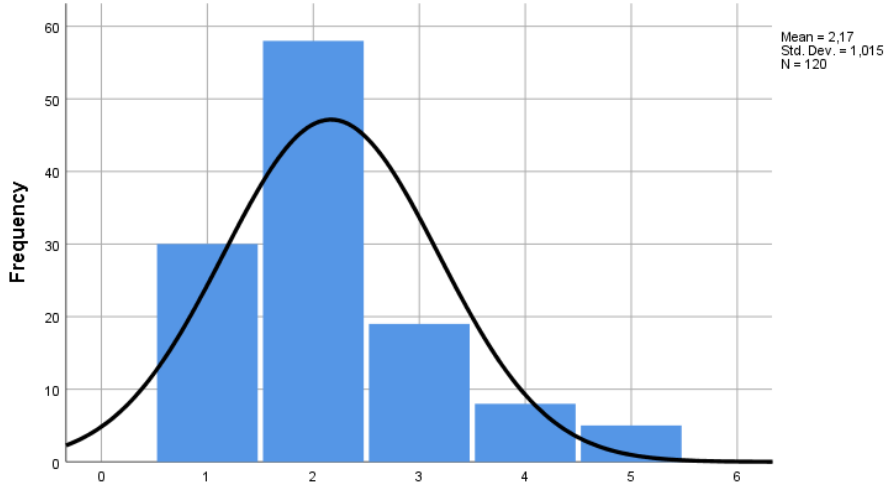
Şekil 3.38: Özel entegratörün, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef ve GİB ile haberleşmesinde kullanılan yazılım uygulamalarının veri tabanı motorları ve uygulama kayıt altına alınmış olması bilgi sistemleri kalitesini artırır.



Katılımcılara denetim izleri yönetimi ilgili ters bir formatta “Denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınması bilgi sistemleri kalitesini artırmaz.” ifadesi sunulmuştur. Katılımcıların %70’inden fazlası bu ifadeye katılmadıklarını yani denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınması bilgi sistemleri kalitesini artırır fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,83$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifade standart sapma açısından denetim izleri yönetimi algısı boyutunun en

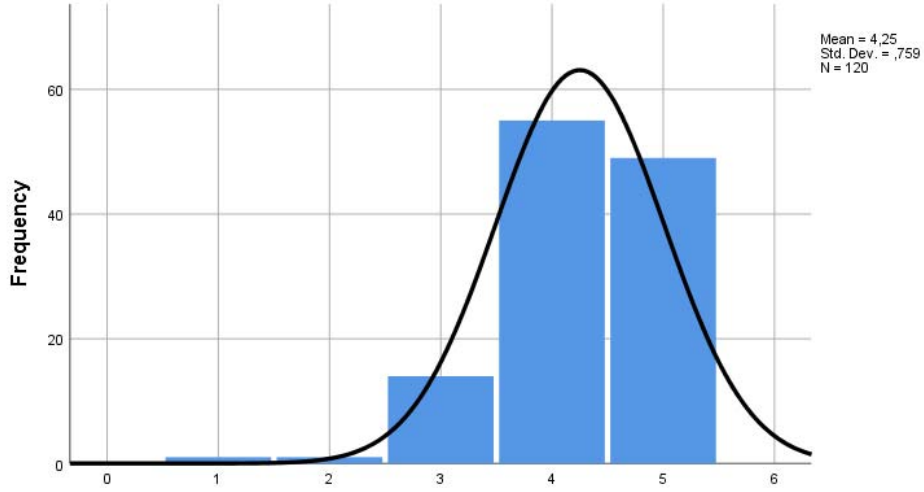
yüksek değerine (SS=1,015) sahip olduğu da görülmektedir. Buna göre, bağımsız denetçiler, denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınması bilgi sistemleri kalitesini artırdığını belirtmektedirler.

Şekil 3.39: Denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınması bilgi sistemleri kalitesini artırmaz.



Araştırmaya katılan katılımcıların “Denetim İzleri yönetimi için veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl oluştuğunun ve saklandığının kayıt altına alınmış olması bilgi sistemleri kalitesini artırır.” ifadesine verdikleri cevaplar %40,8 kesinlikle katılıyorum ve %45,8 katılıyorum şeklindedir. İfadenin ortalamasına bakıldığında ($\bar{X}=4,25$ “kesinlikle katılıyorum”) yüksek bir değer aralığında olduğu belirlenmiştir. Buna göre katılımcıların büyük bir çoğunluğu denetim izleri yönetimi için veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl oluştuğunun ve saklandığının kayıt altına alınmış olması bilgi sistemleri kalitesini artırır fikrine katılmaktadır.

Şekil 3.40: Denetim İzleri yönetimi için veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl oluştuğunun ve saklandığının kayıt altına alınmış olması bilgi sistemleri kalitesini artırır.



Sonuç olarak bağımsız denetçilerin denetim izleri yönetimine ilişkin ifadelerle dair görüşlerinin ortalamasının $\bar{X}=4,07$ ve standart sapmasının $SS=0,759$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin denetim izleri yönetimi raporuna ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.

Aşağıda yer alan Tablo 3.11’de değişiklik yönetimine ilişkin 3 ifade bulunmakta ve katılımcılar tarafından bu ifadelerle verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

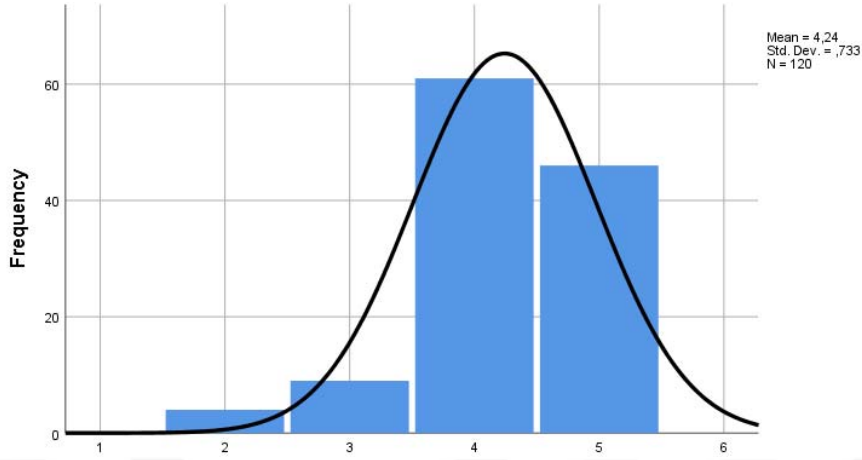
Tablo 3.11: Bağımsız Denetçilerin Değişiklik Yönetimine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)						Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum	Veri Sayısı (n) - (%)		
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz.								
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1. Değişiklik yönetimi prosedüründe, bilgi sistemlerinde yer alan tüm donanım ve yazılımın her türlü bakım, yama ve değişikliğinin kapsamında yer alması bilgi sistemleri kalitesini artırır.	0	4	9	61	46	120	4,24	0,733
2. Özel entegratörün, hizmetlerinde kullandığı, mükellef ve GİB ile entegrasyonu sağlayan yazılımların değişiklik yönetimini yapması bilgi sistemleri kalitesini artırır.	0	5	15	57	43	120	4,15	0,795
3. Değişiklik yönetimi için bir prosedür oluşturulması bilgi sistemleri kalitesini artırır.	1	7	12	54	46	120	4,14	0,882
	0,8	5,8	10,0	45,0	38,3	100		
Ölçeğin Ortalaması ve Standart Sapması							4,17	0,684

Tablo 3.11’de görüldüğü üzere değişiklik yönetimine ilişkin ifadelerle ilgili katılımcıların (1-Kesinlikle Katılmıyorum ve 5-Kesinlikle Katılıyorum aralığında) verdikleri yanıtlar analiz edilmiş ve sonuçlara ulaşılmıştır.

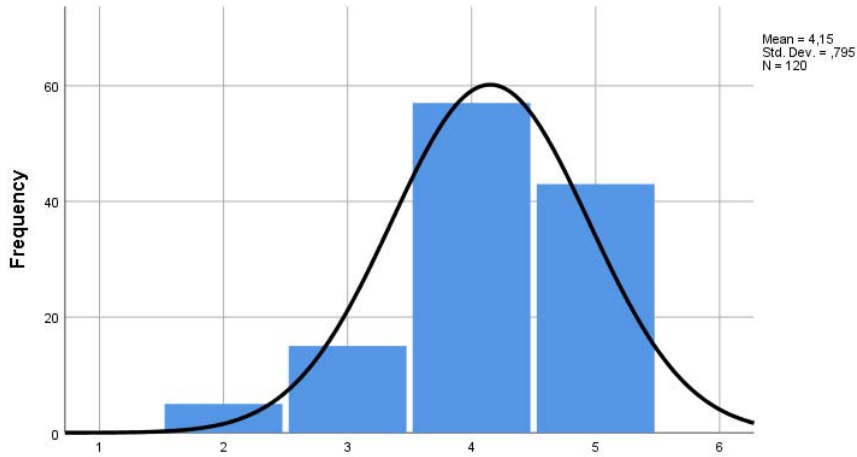
Araştırmaya katılan katılımcıların büyük bir kısmı (%89,1) “Değişiklik yönetimi prosedüründe, bilgi sistemlerinde yer alan tüm donanım ve yazılımın her türlü bakım, yama ve değişikliğinin kapsamında yer alması bilgi sistemleri kalitesini artırır.” ifadesine katıldığı (%50,8=katılıyorum, %38,3= kesinlikle katılıyorum), %7,5’inin kararsız kaldığı görülmektedir. Bu ifadenin ortalamasına bakıldığında (\bar{X} =4,24) değişiklik yönetimine ilişkin boyutun en yüksek ortalamasına sahip olduğu ve ifadenin “kesinlikle katılıyorum” değeri aralığında olduğu görülmektedir.

Şekil 3.41: Değişiklik yönetimi prosedüründe, bilgi sistemlerinde yer alan tüm donanım ve yazılımın her türlü bakım, yama ve değişikliğinin kapsamında yer alması bilgi sistemleri kalitesini artırır.



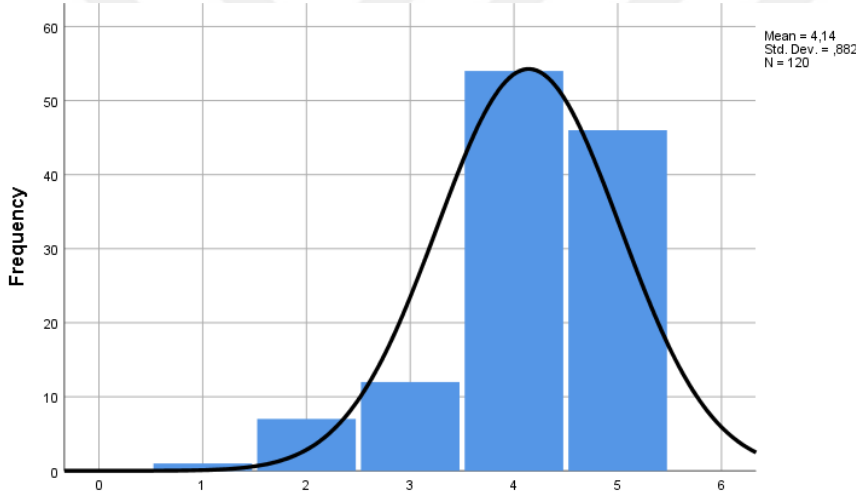
“Özel entegratörün, hizmetlerinde kullandığı, mükellef ve GİB ile entegrasyonu sağlayan yazılımların değişiklik yönetimini yapması bilgi sistemleri kalitesini artırır.” ifadesine katılımcıların %83,3’ü katılmış (%47,5 =katılıyorum, %35,8= kesinlikle katılıyorum), %12,5’i kararsız kalmış, %4,2’si ise katılmamıştır. İfadenin ortalamasına bakıldığında ($\bar{X}=4,15$) yüksek değer aralığında olduğu belirlenmiş ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Buna göre, Özel entegratörün, hizmetlerinde kullandığı, mükellef ve GİB ile entegrasyonu sağlayan yazılımların değişiklik yönetimini yapması bilgi sistemleri kalitesini artırır fikri katılımcılar tarafından yüksek oranda kabul görmektedir.

Şekil 3.42: Özel entegratörün, hizmetlerinde kullandığı, mükellef ve GİB ile entegrasyonu sağlayan yazılımların değişiklik yönetimini yapması bilgi sistemleri kalitesini artırır.



Katılımcılara deęişiklik yönetimine ilişkin “Deęişiklik yönetimi için bir prosedür oluşturulması bilgi sistemleri kalitesini artırır.” ifadesi sunulmuştur. Katılımcıların %81,3’ü bu ifadeye katıldığı (%45=katılıyorum, %38,3=kesinlikle katılıyorum), %10’nun kararsız kaldığı ve geriye kalan %6,6’sının ise katılmadığı görülmektedir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,14$ “katılıyorum”) yüksek bir deęer aralığında olduğu belirlenmiştir. Ayrıca bu ifadenin standart sapma açısından ($SS=0,882$) sahip olduğu görülmektedir. Bu veriler ışığında, katılımcıların büyük çoğunluğunun (%81,3) deęişiklik yönetimi için bir prosedür oluşturulması bilgi sistemleri kalitesini artırır fikrine katıldığı az bir kısmının ise (%6,6) tam tersi bir tutum içerisinde bulunduğu görülmektedir.

Şekil 3.43: Deęişiklik yönetimi için bir prosedür oluşturulması bilgi sistemleri kalitesini artırır.



Sonuç olarak bağımsız denetçilerin deęişiklik yönetimine ilişkin ifadelerle dair görüşlerinin ortalamasının $\bar{X}=4,17$ ve standart sapmasının $SS=0,882$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” deęer aralığında olduğu ve standart sapma deęerinin düşük olduğu görülmektedir. İki deęer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin deęişiklik yönetimi raporuna ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.

Aşağıda yer alan Tablo 3.12’de dış hizmet sağlayıcılarının yönetimine ilişkin 3 ifade bulunmakta ve katılımcılar tarafından bu ifadelerle verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.12: Bağımsız Denetçilerin Dış Hizmet Sağlayıcılarının Yönetimine İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)						Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)							
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum	Veri Sayısı (n) - (%)		
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz.								
1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1. Özel entegratörün, dış hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla denetlemesi bilgi sistemleri kalitesini artırır.	0	3	7	63	47	120	4,28	0,688
2*. Kullanıcıların yaptığı tüm işlemlerin kayıtlarının saklanması bilgi sistemleri kalitesini arturmaz.	1	6	21	53	39	120	4,03	0,884
3.Özel entegratörün dış hizmet alımını sözleşmeye dayalı yapması bilgi sistemleri kalitesini artırır.	1	3	6	95	15	120	4,00	0,594
Ölçeğin Ortalaması ve Standart Sapması							4,10	0,584

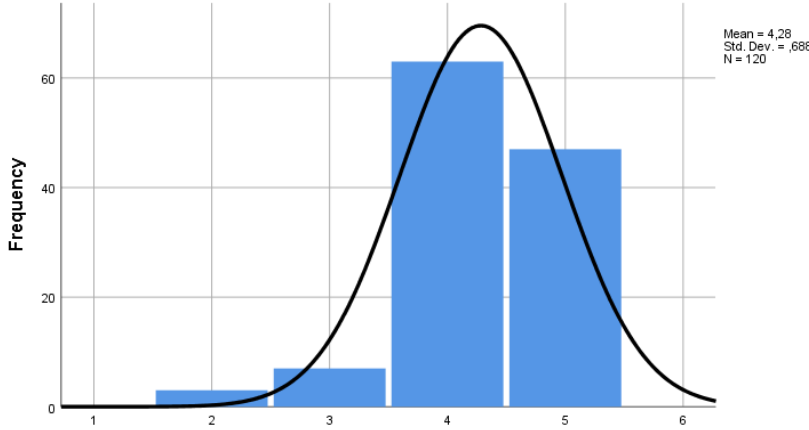
Yukarıdaki tabloda yer alan ifadelere katılımcıların verdikleri yanıtlar analiz edilmiş ve aşağıdaki sonuçlara ulaşılmıştır:

Katılımcılara dış hizmet sağlayıcılarının yönetimine ilişkin ilk çözüm önerisi olarak; “Özel entegratörün, dış hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla denetlemesi bilgi sistemleri kalitesini artırır.” İfadesi sunulmuş ve katılımcıların büyük bir çoğunluğu (%91,7) katıldıklarını (%52,5=katılıyorum, %39,2=kesinlikle katılıyorum), %5,8’i kararsız kaldıklarını ve geriye kalan sadece %2,5’i ise katılmadıklarını belirtmişlerdir. Bu ifadenin aritmetik ortalamasına bakıldığında (\bar{X} =4,28 “kesinlikle katılıyorum”) çok yüksek bir değer aralığında olduğu görülmektedir. Bu veriler doğrultusunda katılımcıların büyük bir çoğunluğu, dış hizmet sağlayıcılarının yönetimine ilişkin olarak; Özel entegratörün, dış

* * Dış Hizmet Sağlayıcılarının Yönetimine İlişkin ifadelerden 2* ters ifadedir. Ters ifadeler analize alınırken SPSS programı üzerinde “Recode into Same Variables” komutu kullanılarak yeniden kodlanmıştır.

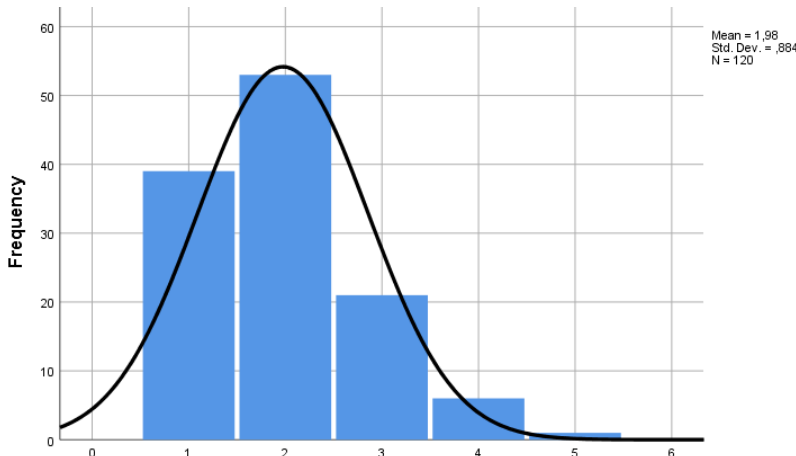
hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla denetlemesi bilgi sistemleri kalitesini artırdığını düşünmektedirler.

Şekil 3.44: Özel entegratörün, dış hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla denetlemesi bilgi sistemleri kalitesini artırır.



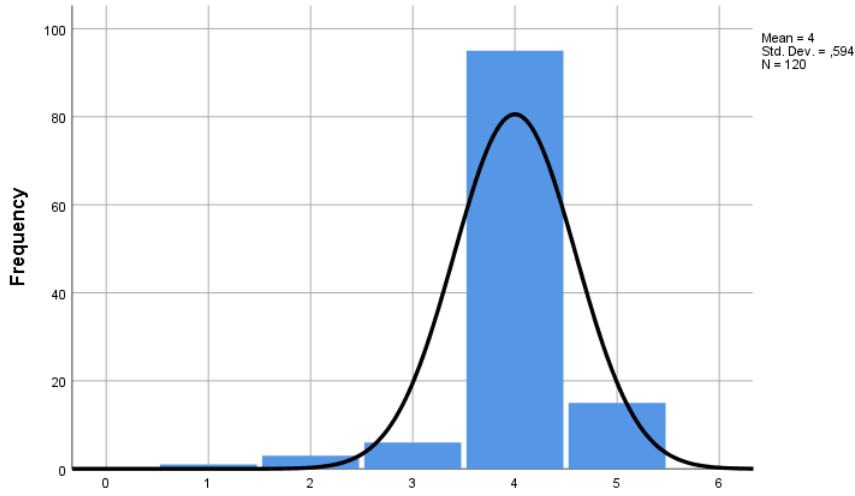
Katılımcılara, dış hizmet sağlayıcılarının yönetimine ilişkin ters bir formatta “Kullanıcıların yaptığı tüm işlemlerin kayıtlarının saklanması bilgi sistemleri kalitesini artırmaz.” ifadesi sunulmuştur. Katılımcıların %76’sından fazlası bu ifadeye katılmadıklarını yani kullanıcıların yaptığı tüm işlemlerin kayıtlarının saklanması bilgi sistemleri kalitesini artırır fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,83$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifade standart sapma açısından dış hizmet sağlayıcılarının yönetimi algısı boyutunun en yüksek değerine ($SS=1,015$) sahip olduğu da görülmektedir.

Şekil 3.45: Kullanıcıların yaptığı tüm işlemlerin kayıtlarının saklanması bilgi sistemleri kalitesini artırmaz.



“Özel entegratörün dış hizmet alımını sözleşmeye dayalı yapması bilgi sistemleri kalitesini artırır.” ifadesine katılımcıların büyük bir kısmı (%91,7) katıldıklarını (%79,2=katılıyorum, %12,5=kesinlikle katılıyorum), %5’i kararsız kaldıklarını belirtmişlerdir. Bu ifadenin aritmetik ortalaması ($\bar{X}=4,03$ “katılıyorum”) yüksek bir değer aralığında olduğu görülmektedir. Dış hizmet sağlayıcılarının yönetimine ilişkin değerlendirmede bu ifadenin standart sapmasının ($\bar{X}=0,594$) en düşük değer aralığında olduğu görülmektedir.

Şekil 3.46: Özel entegratörün dış hizmet alımını sözleşmeye dayalı yapması bilgi sistemleri kalitesini artırır.



Sonuç olarak bağımsız denetçilerin dış hizmet sağlayıcılarının yönetimine ilişkin ifadelerle ilgili görüşlerinin ortalamasının $\bar{X}=4,10$ ve standart sapmasının $SS=0,584$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin denetim izleri yönetimi raporuna ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.

Aşağıda yer alan Tablo 3.13’de hizmet yazılımlarına ilişkin kontrollere ait 4 ifade bulunmakta ve katılımcılar tarafından bu ifadelerle verilen yanıtların frekansları, yüzdeleri, standart sapmaları ve ortalamaları gösterilmektedir.

Tablo 3.13: Bağımsız Denetçilerin Hizmet Yazılımlarına İlişkin İfadelere Dair Görüşlerine Ait Frekans Dağılımları

Ölçek Maddeleri	Frekans (f)						Ortalamalar (\bar{X})	Standart Sapma (SS)
	Yüzde (%)					Veri Sayısı (n) - (%)		
	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum			
Aşağıda yer alan ifadelere katılma düzeyinizi lütfen belirtiniz. 1= Kesinlikle Katılmıyorum 5= Kesinlikle Katılıyorum								
1. Her kullanıcının sadece yetkisi olduğu firma adına fatura gönderebilmesi bilgi sistemleri kalitesini artırır.	2	0	20	64	34	120	4,07	0,775
	1,7	0	16,7	53,3	28,3	100		
2*. Düzenlenen her e-Fatura ve uygulama yanıtında yer alan bilgilerin gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırmaz.	3	11	18	50	38	120	3,91	1,029
	2,5	9,2	15,0	41,7	31,7	100		
3. Düzenlenen her e-Arşiv Fatura, e-SMM, e-MM, e-Bilet vb. altyapıda işleyen elektronik belgeler ve oluşturulan her e-Arşiv raporunda yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.	0	0	11	62	47	120	4,30	0,630
	0	0	9,2	51,7	39,2	100		
4. Düzenlenen her e-İrsaliye ve irsaliye yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.	0	0	9	71	40	120	4,26	0,587
	0	0	7,5	59,2	33,3	100		
Ölçeğin Ortalaması ve Standart Sapması							4,13	0,563

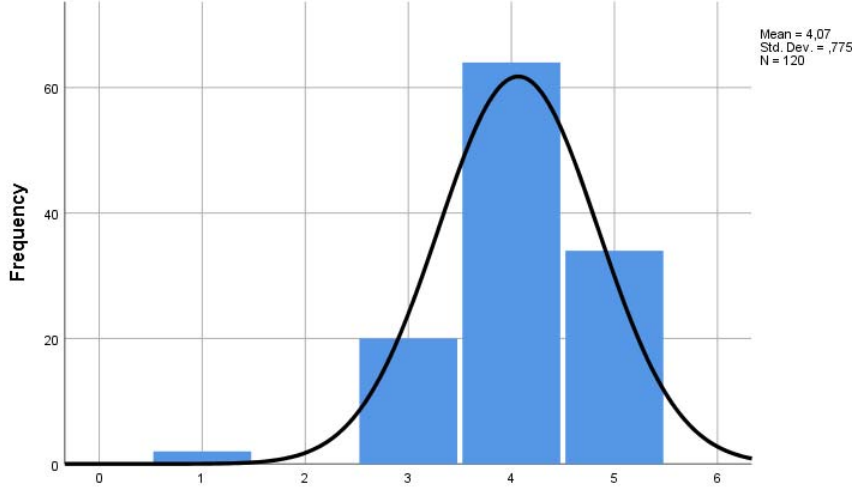
Yukarıdaki tabloda yer alan ifadelere katılımcıların verdikleri yanıtlar analiz edilmiş ve sonuçlara ulaşılmıştır.

Araştırmaya katılan katılımcıların büyük bir kısmı (%81,6) “Her kullanıcının sadece yetkisi olduğu firma adına fatura gönderebilmesi bilgi sistemleri kalitesini artırır.” ifadesine katıldığı (%53,3=katılıyorum, %28,3= kesinlikle katılıyorum), %16,7’sinin

* Hizmet Yazılımlarına İlişkin Kontrollere Ait ifadelerden 2* ters ifadedir. Ters ifadeler analize alınırken SPSS programı üzerinde “Recode into Same Variables” komutu kullanılarak yeniden kodlanmıştır.

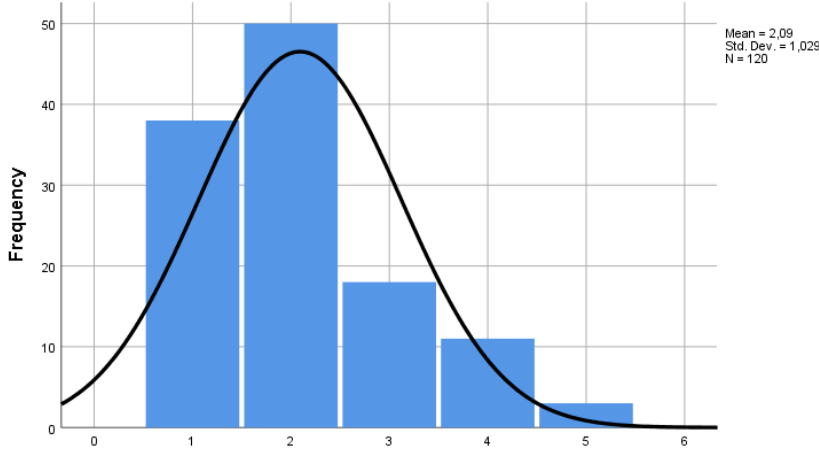
kararsız kaldığı görülmektedir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,07$) ifadenin “katılıyorum” değeri aralığında olduğu görülmektedir.

Şekil 3.47: Her kullanıcının sadece yetkisi olduğu firma adına fatura gönderebilmesi bilgi sistemleri kalitesini artırır.



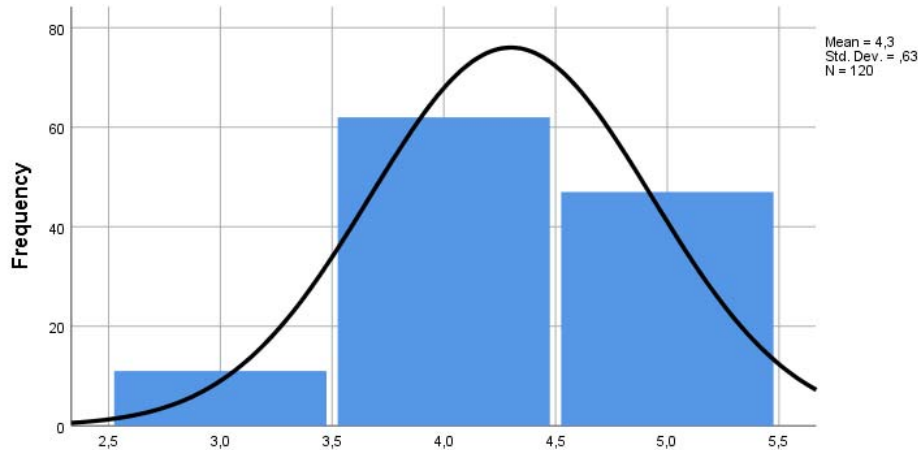
Katılımcılara hizmet yazılımlarına ilişkin kontrollere ait ters bir formatta “Düzenlenen her e-Fatura ve uygulama yanıtında yer alan bilgilerin gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırmaz.” ifadesi sunulmuştur. Katılımcıların %73,4’ü bu ifadeye katılmadıklarını yani düzenlenen her e-fatura ve uygulama yanıtında yer alan bilgilerin gizliliği ve bütünlüğünün korunmasının bilgi sistemleri kalitesini artırır fikrinde oldukları görülmüştür. İfadenin ters kodlanmış şekilde ortalamasına bakıldığında ($\bar{X}=3,91$) katılımcılar bu ifadenin olumlu formatına “katılıyorum” dediği anlaşılmaktadır. Ayrıca bu ifade standart sapma açısından hizmet yazılımlarına ilişkin kontrollere ait ifadenin en yüksek değerine ($SS=1,029$) sahip olduğu da görülmektedir. Buna göre, bağımsız denetçiler, düzenlenen her e-fatura ve uygulama yanıtında yer alan bilgilerin gizliliği ve bütünlüğünün korunmasının bilgi sistemleri kalitesini artırdığını belirtmektedirler.

Şekil 3.48: Düzenlenen her e-Fatura ve uygulama yanıtında yer alan bilgilerin gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.



Katılımcılara gizlilik ve bütünlüğün korunması ile ilgili sunulan; “Düzenlenen her e-Arşiv Fatura, e-SMM, e-MM, e-Bilet vb. altyapıda işleyen elektronik belgeler ve oluşturulan her e-Arşiv raporunda yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.” ifadesine verilen yanıt %51,7 oranında katılıyorum, %39,2 oranında kesinlikle katılıyorum ve %9,2 oranında kararsızım şeklinde olduğu görülmektedir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,30$ “kesinlikle katılıyorum”) en yüksek bir değer aralığında olduğu belirlenmiştir. Ayrıca bu ifade standart sapma açısından ($SS=1,101$) değerine sahip olduğu görülmektedir.

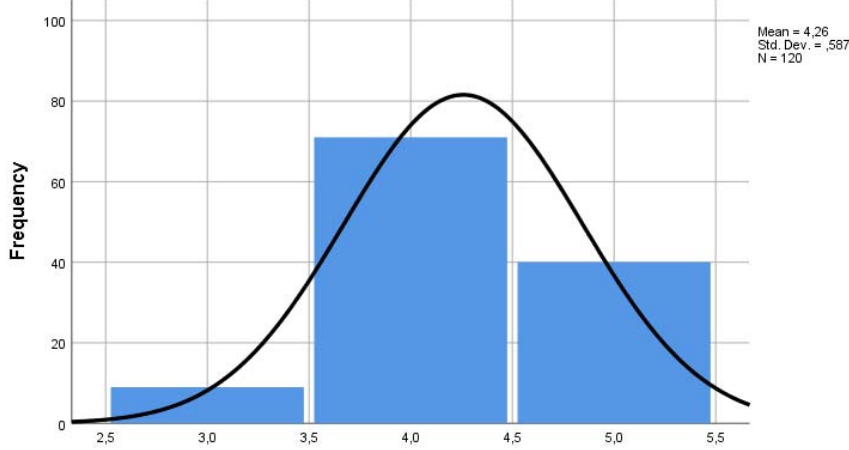
Şekil 3.49: Düzenlenen her e-Arşiv Fatura, e-SMM, e-MM, e-Bilet vb. altyapıda işleyen elektronik belgeler ve oluşturulan her e-Arşiv raporunda yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.



Katılımcılara; “Düzenlenen her e-irsaliye ve irsaliye yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.” ifadesi sunulmuştur. Katılımcıların çok büyük bir kısmının (%92,5) bu ifadeye katıldıklarını yani

düzenlenen her e-İrsaliye ve irsaliye yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunmasının bilgi sistemleri kalitesini artırdığını belirtmişlerdir. Bu ifadenin ortalamasına bakıldığında ($\bar{X}=4,26$) olduğu ve katılımcıların “kesinlikle katılıyorum” dediği anlaşılmaktadır.

Şekil 3.50: Düzenlenen her e-İrsaliye ve irsaliye yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.



Sonuç olarak bağımsız denetçilerin hizmet yazılımlarına ilişkin ifadelerle dair görüşlerinin ortalamasının $\bar{X}=4,26$ ve standart sapmasının $SS=0,587$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “kesinlikle katılıyorum” değer aralığında olduğu ve standart sapma değerinin düşük olduğu görülmektedir. İki değer birlikte ele alındığında araştırmaya katılan bağımsız denetçilerin hizmet yazılımlarına ilişkin kontrollere ait fikirlerinin yüksek seviyede olduğu söylenebilir.

3.7.4. Araştırma Hipotezlerinin Analizleri

Bağımsız Gruplar T Testi

T testi, iki örneklem grubu arasında ortalamalar açısından fark olup olmadığını araştırmak için kullanılır. T testi, bir gruptaki ortalamanın diğer gruptaki ortalamadan önemli derecede farklı olup olmadığını belirler. (Kalaycı, 2017: 74).

Bağımsız gruplar t-testi ise iki bağımsız grubun ortalamalarının birbirinden farklı olup olmadığını test etmek amacıyla kullanılan istatistiksel analiz yöntemidir. Bu testin yapılabilmesi için karşılaştırılacak olan grupların birbirinden bağımsız olması ve bu gruplardan elde edilen ölçümlerin en az eşit aralıklı ölçek düzeyinde ölçülmüş olması gerekmektedir (Durmuş vd., 2016: 118).

Anova Testi

Varyans analizi veya F Testi olarak bilinen Anova testi, grup ortalamaları ve bunlara bağlı olan işlemleri analiz etmek için kullanılan testtir (Gürbüz ve Şahin, 2016: 240). İki'den fazla bağımsız grubun ortalamalarının birbirinden farklı olup olmadığını test etmek amacıyla kullanılan istatistiksel analiz yöntemine tek yönlü varyans analizi denir. Tek yönlü varyans analizinin yapılabilmesi için karşılaştırılacak olan grupların birbirinden bağımsız olması ve bu gruplardan elde edilen ölçümlerin en az eşit aralıklı ölçek düzeyinde ölçülmüş olması gerekmektedir. Bağımsız gruplar t-testinde olduğu gibi tek yönlü varyans analizinde de grupların varyanslarının eşitliği test edilmelidir. Anova yapılabilmesi için grupların varyanslarının homojen yani eşit olması şartı aranır. (Durmuş vd., 2016: 124).

3.7.4.1. Bilgi Sistem Denetimi ile Bağımsız Denetim Arasındaki İlişkiyi Ölçen Hipotezlerin Analizi

H₁: “Bilgi Sistem Denetimi ile Bağımsız Denetim Arasında Anamlı Bir İlişki Vardır.”

Katılımcıların, bilgi sistem denetimi ile bağımsız denetim arasında anlamlı bir ilişki vardır hipotezine ilişkin sorulara verdikleri cevaplara ait analizler yapılmıştır. Tablo 3.14’de bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadelerle ilişkin görüşlerine ait t testi sonuçları yer almaktadır.

Tablo 3.14: Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisine İlişkin İfadelerle Ait Görüşleri

		$\bar{x} \pm S$
Cinsiyet	<i>Kadın</i>	4,0540±,33955
	<i>Erkek</i>	4,0066±,49198
ISACA Tarafından Verilen CISA Belgesine Sahip misiniz?	<i>Evet</i>	4,0993±,46982
	<i>Hayır</i>	4,0115±,43757
Yaş	<i>30 ve altı</i>	3,8661±,46152
	<i>30-39</i>	3,9297±,40944
	<i>40-49</i>	4,0387±,44771
	<i>50-59</i>	4,1563±,43536
	<i>60 ve üzeri</i>	4,0846±,40801
Eğitim durumu	<i>Lisans</i>	3,9927±,45857
	<i>Yüksek Lisans</i>	4,0401±,43164
	<i>Doktora</i>	4,1696±,37796

Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,9303±,43260
	<i>6-10 yıl</i>	4,0430±,42875
	<i>11-15 yıl</i>	4,0096±,54477
	<i>16 yıl ve üzeri</i>	4,2174±,37161
Denetim Firmasındaki Pozisyonu	<i>Denetçi</i>	3,8815±,38612
	<i>Yardımcısı</i>	
	<i>Denetçi</i>	4,1182±,41739
	<i>Kıdemli Denetçi</i>	3,8750±,47425
	<i>Baş Denetçi</i>	4,2941±,39266
	<i>Sorumlu Ortak Baş Denetçi</i>	3,9669±,45614
Ölçeğin Ortalaması ve Standart Sapması		4,020±,441

Sonuç olarak “Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere İlişkin Görüşlerine Ait Frekans Dağılımları” incelendiğinde ortalamanın $\bar{X}=4,02$ değerini aldığı ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Standart sapma değeri ise $SS=0,441$ olarak bulunmuş ve bu değer düşük olduğu görülmektedir. Bu iki değer birlikte incelendiğinde bağımsız denetçilere göre bilgi sistemleri denetiminin bağımsız denetime etkisinin olduğu ve bu etkinin yüksek seviyede olduğu söylenebilir. Dolayısıyla “*Bilgi sistem denetimi ile bağımsız denetim arasında anlamlı bir ilişki vardır*” hipotezi kabul edilmiştir.

H₂: “Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Cinsiyetlerine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisine ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini görebilmek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.15’ de yer almaktadır.

Tablo 3.15: Cinsiyete Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisine İlişkin İfadelere Ait Görüşleri İçin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,1733±0,37448	0,625	0,533
	<i>Erkek</i>	4,1176±0,51760		

Analiz sonucunda kadın grubu ($\bar{x}=4,1733$, $S=0,37448$) ile erkek grubu ($\bar{x}=4,1176$, $S=0,51760$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir

fark tespit edilmemiştir ($t_{(118)}=0,625$; $p=0,543$). “Cinsiyete Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Farklılaşmaktadır” hipotezi reddedilmiştir.

H₃: “Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini görebilmek için 120 kişiden elde edilen verilere bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.25’ de yer almaktadır.

Tablo 3.16: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi İlişkin İfadelere Ait Görüşleri İçin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
ISACA tarafından verilen CISA belgesine sahip olma durumu	<i>Evet</i>	4,2353±,49040	0,922	0,358
	<i>Hayır</i>	4,1220±,46626		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,2353$, $S=0,49040$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,1220$, $S=0,46626$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,922$; $p=0,358$). “ISACA tarafından verilen CISA belgesine sahip olma durumuna göre bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri farklılaşmaktadır” hipotezi reddedilmiştir.

H₄: “Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadelerine dair görüşlerinin, yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.17: Yaş Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelerine Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Yaş	<i>30 ve altı</i>	3,9911±0,44690	1,332	,262
	<i>30-39</i>	4,0234±0,44714		
	<i>40-49</i>	4,1548±0,48358		
	<i>50-59</i>	4,2708±0,49989		
	<i>60 ve üzeri</i>	4,1985±0,41236		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=3,9911$, $S=0,44690$), 30-39 arası yaş grupları ($\bar{x}=4,0234$, $S=0,44714$), 40-49 arası yaş grupları ($\bar{x}=4,1548$, $S=0,48358$), 50-59 arası yaş grupları ($\bar{x}=4,2708$, $S=0,49989$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,1985$, $S=0,41236$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,332$; $p=0,262$). “Yaş durumuna göre bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri farklılaşmaktadır” hipotezi reddedilmiştir.

H₅: “Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadelerine dair görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.18: Eğitim Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile ilgili ifadelerine Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	4,1021±0,49346	,538	,585
	<i>Yüksek Lisans</i>	4,1604±0,44575		
	<i>Doktora</i>	4,2768±0,46049		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1021$, $S=0,49346$), yüksek lisans mezunları ($\bar{x}=4,1604$, $S=0,44575$), doktora mezunları ($\bar{x}=4,2768$, $S=0,46049$) arasında

istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,538$; $p=0,585$). “Eğitim Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Farklılaşmaktadır” hipotezi reddedilmiştir.

H₆: Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.

Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadelerine dair görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır. Tablo 3.19’da tek yönlü varyans analizi sonuçları görülmektedir.

Tablo 3.19: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelerine Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	4,0313±0,46483	2,525	,061
	<i>6-10 yıl</i>	4,1816±0,43947		
	<i>11-15 yıl</i>	4,1010±0,57199		
	<i>16 yıl ve üzeri</i>	4,3397±0,40846		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=4,0313$, $S=0,46483$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,1816$ $S=0,43947$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,1010$, $S=0,40846$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,3397$, $S=0,40846$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=2,525$; $p=0,061$). “Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Farklılaşmaktadır” hipotezi reddedilmiştir.

H₇: “Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadelerle dair görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.20: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelerle Dair Görüşlerine İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,9741±0,38292	3,666	,008
	<i>Denetçi</i>	4,2534±0,46139		
	<i>Kıdemli Denetçi</i>	3,9969±0,46660		
	<i>Baş Denetçi</i>	4,4044±0,42798		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0662±0,52500		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=3,9741$, $S=0,38292$), denetçi olanlar ($\bar{x}=4,2534$, $S=0,46139$), kıdemli denetçi olanlar ($\bar{x}=3,9969$, $S=0,46660$), baş denetçi olanlar ($\bar{x}=4,4044$, $S=0,42798$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,0662$, $S=0,52500$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=3,666$; $p=0,008$). “Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili Görüşleri Farklılaşmaktadır” hipotezi kabul edilmiştir.

Tablo 3.21: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>Denetçi Yardımcısı</i>	<i>Denetçi</i>	<i>Kıdemli Denetçi</i>	<i>Baş Denetçi</i>	<i>Sorumlu Ortak Baş Denetçi</i>
<i>Denetçi Yardımcısı</i>		,097	1,000	,018	,962
<i>Denetçi</i>	,097		,247	,781	,615
<i>Kıdemli Denetçi</i>	1,000	,247		,053	,990
<i>Baş Denetçi</i>	,018	,781	,053		,190
<i>Sorumlu Ortak Baş Denetçi</i>	,962	,615	,990	,190	

Denetim firmasındaki pozisyonu için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın denetçi yardımcısı ($\bar{x}=3,9741$, $S=0,38292$) ile baş denetçi ($\bar{x}=4,4044$, $S=0,42798$) arasında olduğu görülmüştür ($p=0,008$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi

yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,018$). Bu sonuç baş denetçilerin “bilgi sistemleri denetiminin bağımsız denetime etkisi” olduğu fikrine denetçi yardımcılara göre daha fazla katıldıklarını göstermektedir. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

3.7.4.2. Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeylerini Ölçmeye Yönelik Hipotezlerin Analizi

H₈: “Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Yükseklerdir.”

Katılımcıların, “bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri yüksektir” hipotezine ilişkin sorulara verdikleri cevaplara ait analizler yapılmıştır. Tablo 3.22’de bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadelerle ilişkin görüşlerine ait t testi sonuçları yer almaktadır.

Tablo 3.22: Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri ile İlgili İfadelerle Ait Görüşleri

Bağımsız Örneklem T Testi		$\bar{x} \pm S$
Cinsiyet	<i>Kadın</i>	4,1076±,42638
	<i>Erkek</i>	4,0789±,48442
ISACA Tarafından Verilen CISA Belgesine Sahip misiniz?	<i>Evet</i>	4,3216±,41011
	<i>Hayır</i>	4,0511±,46105
Yaş	<i>30 ve altı</i>	4,1127±,36385
	<i>30-39</i>	3,9938±,45268
	<i>40-49</i>	4,0397±,52012
	<i>50-59</i>	4,1681±,44586
	<i>60 ve üzeri</i>	4,1627±,47124
Eğitim durumu	<i>Lisans</i>	4,1006±,53508
	<i>Yüksek Lisans</i>	4,0704±,37863
	<i>Doktora</i>	4,1381±,41830
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,9321±,45652
	<i>6-10 yıl</i>	4,1156±,43823
	<i>11-15 yıl</i>	4,2513±,47446
	<i>16 yıl ve üzeri</i>	4,3174±,38793
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,9575±,40998
	<i>Denetçi</i>	4,0613±,47626

	<i>Kıdemli Denetçi</i>	4,0483±,38044
	<i>Baş Denetçi</i>	4,4176±,36307
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0961±,57601
Ölçeğin Ortalaması ve Standart Sapması		4,0894±,46236

Sonuç olarak “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri ile ilgili ifadelerle ait görüşlerin frekans dağılımları” incelendiğinde ortalamanın $\bar{X}=4,0894$ değerini aldığı ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Standart sapma değeri ise $SS=0,46236$ olarak bulunmuş ve bu değer düşük olduğu görülmektedir. Bu iki değer birlikte incelendiğinde bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerinin yüksek seviyede olduğu söylenebilir. Dolayısıyla “*Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Yüksek*” hipotezi kabul edilmiştir.

H₉: “Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin, görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini görebilmek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.23’ de yer almaktadır.

Tablo 3.23: Cinsiyete Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin İfadelerle Ait Görüşleri İçin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,1076±,42638	,326	,745
	<i>Erkek</i>	4,0789±,48442		

Analiz sonucunda kadın grubu ($\bar{x}=4,1076$, $S=0,42638$) ile erkek grubu ($\bar{x}=4,0789$, $S=0,48442$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,326$; $p=0,745$). “*Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklılaşmaktadır*” hipotezi reddedilmiştir.

H_{9.1}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.24’ de yer almaktadır.

Tablo 3.24: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelere dair görüşlerine ilişkin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,1989±,38722	0,610	0,543
	<i>Erkek</i>	4,1447±,50870		

Analiz sonucunda kadın grubu ($\bar{x}=4,1989$, $S=0,38722$) ile erkek grubu ($\bar{x}=4,1447$, $S=0,50870$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,610$; $p=0,543$). Yani bu hipotez reddedilmiştir.

H_{9.2}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.25’de yer almaktadır.

Tablo 3.25: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,1061±,60903	,078	,938
	<i>Erkek</i>	4,0965±,66626		

Analiz sonucunda kadın grubu ($\bar{x}=4,1061$, $S=0,60903$) ile erkek grubu ($\bar{x}=4,0965$, $S=0,66626$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,078$; $p=0,938$). Yani bu hipotez reddedilmiştir.

H_{9,3}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.26’ da yer almaktadır.

Tablo 3.26: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,1420±,49825	-,169	,866
	<i>Erkek</i>	4,1612±,64641		

Analiz sonucunda kadın grubu ($\bar{x}=4,1420$, $S=0,49825$) ile erkek grubu ($\bar{x}=4,1612$, $S=0,64641$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=-0,169$; $p=0,866$).

H_{9,4}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.27’ de yer almaktadır.

Tablo 3.27: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	3,9545±,59538	,092	,927
	<i>Erkek</i>	3,9430±,69578		

Analiz sonucunda kadın grubu ($\bar{x}=3,9545$, $S=0,59538$) ile erkek grubu ($\bar{x}=3,9430$, $S=0,69578$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,092$; $p=0,927$). Yani bu hipotez reddedilmiştir.

H_{9.5}: “Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBS D değerlendirme sınıflarından erişim güvenliği raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.28’de yer almaktadır.

Tablo 3.28: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	3,9394±,64808	,439	,661
	<i>Erkek</i>	3,8860±,63841		

Analiz sonucunda kadın grubu ($\bar{x}=3,9394$, $S=0,64808$) ile erkek grubu ($\bar{x}=3,8860$, $S=0,63841$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,439$; $p=0,661$). Yani bu hipotez reddedilmiştir.

H_{9.6}: “Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBS D değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına

bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.29’ da yer almaktadır.

Tablo 3.29: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,1288±,63170	,668	,505
	<i>Erkek</i>	4,0395±,74430		

Analiz sonucunda kadın grubu ($\bar{x}=4,1288$, $S=0,63170$) ile erkek grubu ($\bar{x}=4,0395$, $S=0,74430$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,668$; $p=0,505$). Yani bu hipotez reddedilmiştir.

H_{9,7}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelere ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.30’ da yer almaktadır.

Tablo 3.30: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,0833±,52888	,071	,943
	<i>Erkek</i>	4,0746±,70888		

Analiz sonucunda kadın grubu ($\bar{x}=4,0833$, $S=0,52888$) ile erkek grubu ($\bar{x}=4,0746$, $S=0,70888$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,071$; $p=0,943$). Yani bu hipotez reddedilmiştir.

H_{9,8}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından değişiklik yönetimi raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.31’ de yer almaktadır.

Tablo 3.31: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,1970±,57654	,233	,816
	<i>Erkek</i>	4,1667±,74337		

Analiz sonucunda kadın grubu ($\bar{x}=4,1970$, $S=0,57654$) ile erkek grubu ($\bar{x}=4,1667$, $S=0,74337$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,233$; $p=0,816$). Yani bu hipotez reddedilmiştir.

H_{9,9}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.32’ de yer almaktadır.

Tablo 3.32: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,0985±,53594	-,061	,951
	<i>Erkek</i>	4,1053±,61394		

Analiz sonucunda kadın grubu ($\bar{x}=4,0985$, $S=0,53594$) ile erkek grubu ($\bar{x}=4,1053$, $S=0,61394$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=-0,061$; $p=0,951$). Yani bu hipotez reddedilmiştir.

H_{9,10}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Cinsiyetlerine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller raporu ile ilgili ifadelerle ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.33 ‘de yer almaktadır.

Tablo 3.33: Cinsiyete Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,1364±,49254	,045	,964
	<i>Erkek</i>	4,1316±,60343		

Analiz sonucunda kadın grubu ($\bar{x}=4,1364$, $S=0,49254$) ile erkek grubu ($\bar{x}=4,1316$, $S=0,60343$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,045$; $p=0,964$). Yani bu hipotez reddedilmiştir.

H₁₀: “Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin CISA belgesine sahip olup olmama durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan t testi sonuçları aşağıda yer almaktadır.

Tablo 3.34: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
ISACA tarafından verilen CISA belgesine sahip misiniz ?	<i>Evet</i>	4,3216±,41011	2,273	,025
	<i>Hayır</i>	4,0511±,46105		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,3216$, $S=0,41011$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,0511$, $S=0,46105$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmiştir ($t=2,273$; $p=0,025$). “ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Farklılaşmaktadır” hipotezi kabul edilmiştir.

H_{10.1}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini görebilmek için 120 kişiden elde edilen verilere bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.35’de yer almaktadır.

Tablo 3.35: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
ISACA tarafından verilen CISA belgesine sahip olma durumu	<i>Evet</i>	4,3971±,38587	2,254	0,026
	<i>Hayır</i>	4,1262±,46950		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,3971$, $S=0,38587$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,1220$, $S=0,46626$) arasında fikir düzeyleri

ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,922$; $p=0,358$). Yani bu hipotez reddedilmiştir.

H_{10.2}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelerle ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini görebilmek için 120 kişiden elde edilen verilere bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.36’da yer almaktadır.

Tablo 3.36: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
ISACA tarafından verilen CISA belgesine sahip olma durumu	<i>Evet</i>	4,4510±,49918	2,480	0,015
	<i>Hayır</i>	4,0421±,64791		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,4510$, $S=0,49918$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,0421$, $S=0,64791$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmiştir ($t_{(118)}=2,480$; $p=0,015$). Bu hipotez kabul edilmiştir.

H_{10.3}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.37’de yer almaktadır.

Tablo 3.37: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,2059±,68599	,386	,700
	<i>Erkek</i>	4,1456±,58108		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,2059$, $S=0,68599$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,1456$, $S=0,58108$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,386$; $p=0,700$). Yani bu hipotez reddedilmiştir.

H_{10.4}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.38’de yer almaktadır.

Tablo 3.38: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,3725±,51211	2,969	,004
	<i>Erkek</i>	3,8770±,65511		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,3725$, $S=0,51211$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=3,8770$, $S=0,65511$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmiştir ($t_{(118)}=2,969$; $p=0,004$). Bu hipotez kabul edilmiştir.

H_{10.5}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından erişim güvenliği raporu ile ilgili ifadelerle ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.39’ da yer almaktadır.

Tablo 3.39: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,0784±,67216	1,205	,231
	<i>Erkek</i>	3,8770±,63313		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,0784$, $S=0,67216$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=3,8770$, $S=0,63313$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=1,205$; $p=0,231$). Yani bu hipotez reddedilmiştir.

H_{10.6}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları raporu ile ilgili ifadelerle ilişkin, katılımcıların ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.40’da yer almaktadır.

Tablo 3.40: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,1961±,82545	,782	,436
	<i>Erkek</i>	4,0518±,68402		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,1961$, $S=0,82545$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,0518$, $S=0,68402$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,732$; $p=0,436$). Yani bu hipotez reddedilmiştir.

H_{10.7}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Denetim İzleri Yönetimi Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.41’de yer almaktadır.

Tablo 3.41: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Denetim İzleri Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,2745±,63722	1,359	,177
	<i>Erkek</i>	4,0453±,64516		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,2745$, $S=0,63722$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,0453$, $S=0,64516$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=1,359$; $p=0,177$). Yani bu hipotez reddedilmiştir.

H_{10.8}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere İlişkin İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından değişiklik yönetimi raporu ile ilgili ifadelerle ilişkin, katılımcıların ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.42’de yer almaktadır.

Tablo 3.42: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

Bağımsız Örneklem T Testi		$\bar{x} \pm S$	T	P değeri
Cinsiyet	<i>Kadın</i>	4,3725±,73487	,666	,207
	<i>Erkek</i>	4,1456±,67425		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,3725$, $S=0,73487$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,1456$, $S=0,67425$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=0,666$; $p=0,207$). Yani bu hipotez reddedilmiştir.

H_{10.9}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.43’de yer almaktadır.

Tablo 3.43: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,2353±,69487	1,009	,315
	<i>Erkek</i>	4,0809±,56489		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,2353$, $S=0,69487$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,0809$, $S=0,56489$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmemiştir ($t_{(118)}=1,009$; $p=0,315$). Yani bu hipotez reddedilmiştir.

H_{10.10}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin, katılımcıların ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için cinsiyet gruplarına bağımsız örneklem t-testi yapılmıştır. Bağımsız örneklem t-testi sonuçları Tablo 3.44’de yer almaktadır.

Tablo 3.44: ISACA Tarafından Verilen CISA Belgesine Sahip Olma Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere Dair Görüşlerine İlişkin T Testi Sonuçları

<i>Bağımsız Örneklem T Testi</i>		$\bar{x} \pm S$	T	<i>P değeri</i>
Cinsiyet	<i>Kadın</i>	4,4118±,57242	2,237	,027
	<i>Erkek</i>	4,0874±,55097		

Analiz sonucunda evet cevabı veren bağımsız denetçiler ($\bar{x}=4,4118$, $S=0,57242$) ile hayır cevabı veren bağımsız denetçiler ($\bar{x}=4,0874$, $S=0,55097$) arasında fikir düzeyleri ortalamaları açısından istatistiksel olarak anlamlı bir fark tespit edilmiştir ($t_{(118)}=2,237$; $p=0,027$). Hipotez kabul edilmiştir.

H₁₁: “Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin yaş durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi sonuçları aşağıda yer almaktadır.

Tablo 3.45: Yaş Durumuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Yaş	30 ve altı	4,1127±,36385	,578	,679
	30-39	3,9938±,45268		
	40-49	4,0397±,52012		
	50-59	4,1681±,44586		
	60 ve üzeri	4,1627±,47124		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,1127$, $S=0,36385$), 30-39 arası yaş grupları ($\bar{x}=3,9938$, $S=0,45268$), 40-49 arası yaş grupları ($\bar{x}=4,0397$, $S=0,52012$), 50-59 arası yaş grupları ($\bar{x}=4,1681$, $S=0,44586$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,1627$, $S=0,47124$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,578$; $p=0,679$). “Yaş durumuna göre bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri farklılaşmaktadır” hipotezi reddedilmiştir.

H_{11.1}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile ilgili İfadelerine İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.46: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile ilgili İfadelerine İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Yaş	<i>30 ve altı</i>	4,1905±,23591	,336	,853
	<i>30-39</i>	4,0625±,49582		
	<i>40-49</i>	4,1429±,54421		
	<i>50-59</i>	4,2083±,44640		
	<i>60 ve üzeri</i>	4,2206±,50685		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,1905$, $S=0,23591$), 30-39 arası yaş grupları ($\bar{x}=4,0625$, $S=0,49582$), 40-49 arası yaş grupları ($\bar{x}=4,1429$, $S=0,54421$), 50-59 arası yaş grupları ($\bar{x}=4,2083$, $S=0,44640$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,2206$, $S=0,50685$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,336$; $p=0,853$). Yani bu hipotez reddedilmiştir.

H_{11.2}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile ilgili ifadelerle İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerle ilişkin, katılımcıların yaşına göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.47: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme sınıflarından İç Kontrol ve Denetim Mekanizmaları Raporu ile ilgili ifadelerle İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Yaş	<i>30 ve altı</i>	4,1905±,40237	1,484	,212
	<i>30-39</i>	3,8542±,67735		
	<i>40-49</i>	4,0079±,74167		
	<i>50-59</i>	4,2083±,65062		
	<i>60 ve üzeri</i>	4,2941±,52549		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,1905$, $S=0,40237$), 30-39 arası yaş grupları ($\bar{x}=3,8542$, $S=0,67735$), 40-49 arası yaş grupları ($\bar{x}=4,0079$, $S=0,4167$), 50-59 arası yaş grupları ($\bar{x}=4,2083$, $S=0,65062$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,2941$,

S=0,52549) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır (F=1,484; $p=0,212$). Yani bu hipotez reddedilmiştir.

H_{11.3}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.48: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Yaş	<i>30 ve altı</i>	4,0000±,57009	0,716	,583
	<i>30-39</i>	4,1563±,57645		
	<i>40-49</i>	4,1310±,59274		
	<i>50-59</i>	4,2917±,58823		
	<i>60 ve üzeri</i>	4,2059±,66869		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,0000$, S=0,57009), 30-39 arası yaş grupları ($\bar{x}=4,1563$ S=0,57645), 40-49 arası yaş grupları ($\bar{x}=4,1310$, S=0,59274), 50-59 arası yaş grupları ($\bar{x}=4,2917$, S=0,58823), 60 ve üzeri arası yaş grupları ($\bar{x}=4,2059$, S=0,66869) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır (F=0,716; $p=0,583$). Yani bu hipotez reddedilmiştir.

H_{11.4}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.49: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Yaş	<i>30 ve altı</i>	4,0159±,54238	0,263	,901
	<i>30-39</i>	3,8750±,78764		
	<i>40-49</i>	3,9127±,76530		
	<i>50-59</i>	3,9167±,52244		
	<i>60 ve üzeri</i>	4,0588±,59202		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,0159$, $S=0,54238$), 30-39 arası yaş grupları ($\bar{x}=3,8750$ $S=0,78764$), 40-49 arası yaş grupları ($\bar{x}=3,9127$, $S=0,76530$), 50-59 arası yaş grupları ($\bar{x}=3,9167$, $S=0,52244$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,0588$, $S=0,59202$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,716$; $p=0,583$). Yani bu hipotez reddedilmiştir.

H_{11.5}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.50: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Yaş	<i>30 ve altı</i>	4,0794±,65748	0,539	,708
	<i>30-39</i>	3,8333±,60858		
	<i>40-49</i>	3,8413±,65947		
	<i>50-59</i>	3,9028±,55149		
	<i>60 ve üzeri</i>	3,9216±,74096		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,0794$, $S=0,65748$), 30-39 arası yaş grupları ($\bar{x}=3,8333$ $S=0,60858$), 40-49 arası yaş grupları ($\bar{x}=3,8413$, $S=0,65947$), 50-59 arası yaş grupları ($\bar{x}=3,9028$, $S=0,55149$), 60 ve üzeri arası yaş grupları ($\bar{x}=3,9216$,

S=0,74069) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır (F=0,539; $p=0,708$). Yani bu hipotez reddedilmiştir.

H_{11.6}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.51: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları Raporu ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Yaş	<i>30 ve altı</i>	4,1746±,51228	1,265	,288
	<i>30-39</i>	3,8542±,75000		
	<i>40-49</i>	3,9683±,75371		
	<i>50-59</i>	4,2778±,71334		
	<i>60 ve üzeri</i>	4,1176±,69663		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,1746$, S=0,51228), 30-39 arası yaş grupları ($\bar{x}=3,8542$ S=0,75000), 40-49 arası yaş grupları ($\bar{x}=3,9683$, S=0,75371), 50-59 arası yaş grupları ($\bar{x}=4,2778$, S=0,71334), 60 ve üzeri arası yaş grupları ($\bar{x}=4,1176$, S=0,69663) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır (F=1,265; $p=0,288$). Yani bu hipotez reddedilmiştir.

H_{11.7}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.52: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Yaş	<i>30 ve altı</i>	3,9365±,82070	0,465	,761
	<i>30-39</i>	4,0625±,57373		
	<i>40-49</i>	4,0635±,70322		
	<i>50-59</i>	4,1806±,48133		
	<i>60 ve üzeri</i>	4,1569±,55425		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=3,9365$, $S=0,82070$), 30-39 arası yaş grupları ($\bar{x}=4,0625$ $S=0,57373$), 40-49 arası yaş grupları ($\bar{x}=4,0635$, $S=0,70322$), 50-59 arası yaş grupları ($\bar{x}=4,1806$, $S=0,48133$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,1569$, $S=0,55425$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,465$; $p=0,761$). Yani bu hipotez reddedilmiştir.

H_{11.8}: “Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBS D değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.53: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Yaş	<i>30 ve altı</i>	4,0000±,57735	0,452	,771
	<i>30-39</i>	4,2083±,70842		
	<i>40-49</i>	4,2222±,76035		
	<i>50-59</i>	4,1806±,68086		
	<i>60 ve üzeri</i>	4,2549±,62948		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,0000$, $S=0,57735$), 30-39 arası yaş grupları ($\bar{x}=4,2083$ $S=0,70842$), 40-49 arası yaş grupları ($\bar{x}=4,2222$, $S=0,76035$), 50-59 arası yaş grupları ($\bar{x}=4,1806$, $S=0,68086$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,2549$,

S=0,62948) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır (F=0,452; p=0,771). Yani bu hipotez reddedilmiştir.

H_{11.9}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.54: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Yaş	<i>30 ve altı</i>	4,0952±,55919	0,156	,960
	<i>30-39</i>	4,0417±,64262		
	<i>40-49</i>	4,0952±,67589		
	<i>50-59</i>	4,1806±,43936		
	<i>60 ve üzeri</i>	4,0784±,54683		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,0952$, S=0,55919), 30-39 arası yaş grupları ($\bar{x}=4,0417$ S=0,64262), 40-49 arası yaş grupları ($\bar{x}=4,0952$, S=0,67589), 50-59 arası yaş grupları ($\bar{x}=4,1806$, S=0,43936), 60 ve üzeri arası yaş grupları ($\bar{x}=4,0784$, S=0,54683) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır (F=0,156; p=0,960). Yani bu hipotez reddedilmiştir.

H_{11.10}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Yaş Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin görüşlerinin yaşa göre anlamlı bir farklılık

gösterip göstermediğini belirlemek için yaş gruplarına tek yönlü varyans analizi yapılmıştır.

Tablo 3.55: Yaş Durumuna Göre Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller Raporu ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Yaş	<i>30 ve altı</i>	4,1071±,37559	1,066	,376
	<i>30-39</i>	4,0313±,61830		
	<i>40-49</i>	4,0476±,66083		
	<i>50-59</i>	4,3021±,47765		
	<i>60 ve üzeri</i>	4,2353±,54105		

Analiz sonucunda 30 ve altı yaş grupları ($\bar{x}=4,1071$, $S=0,37559$), 30-39 arası yaş grupları ($\bar{x}=4,0313$ $S=0,61830$), 40-49 arası yaş grupları ($\bar{x}=4,0476$, $S=0,66083$), 50-59 arası yaş grupları ($\bar{x}=4,3021$, $S=0,47765$), 60 ve üzeri arası yaş grupları ($\bar{x}=4,2353$, $S=0,54105$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,066$; $p=0,376$). Yani bu hipotez reddedilmiştir.

H₁₂: “Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi sonuçları aşağıda yer almaktadır.

Tablo 3.56: Eğitim Durumuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim durumu	<i>Lisans</i>	4,1006±,53508	,099	,906
	<i>Yüksek Lisans</i>	4,0704±,37863		
	<i>Doktora</i>	4,1381±,41830		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1006$, $S=0,53508$), yüksek lisans mezunları ($\bar{x}=4,0704$, $S=0,37863$), doktora mezunları ($\bar{x}=4,1381$, $S=0,41830$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,099$; $p=0,906$). “Eğitim

Durumuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Farklılaşmaktadır” hipotezi reddedilmiştir.

H_{12.1}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.57: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	4,1625±,52647	,256	,775
	<i>Yüksek Lisans</i>	4,1509±,38085		
	<i>Doktora</i>	4,2857±,56695		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1625$, $S=0,52647$), yüksek lisans mezunları ($\bar{x}=4,1509$, $S=0,38085$), doktora mezunları ($\bar{x}=4,2857$, $S=0,56695$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,256$; $p=0,775$). Yani bu hipotez reddedilmiştir.

H_{12.2}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerine ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.58: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından İ Kontrol ve Denetim Mekanizmaları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	4,0278±,70321	1,041	,356
	<i>Yüksek Lisans</i>	4,1950±,58992		
	<i>Doktora</i>	4,0000±,43033		

Analiz sonucunda lisans mezunları ($\bar{x}=4,0278$, $S=0,70321$), yüksek lisans mezunları ($\bar{x}=4,1950$, $S=0,58992$), doktora mezunları ($\bar{x}=4,0000$, $S=0,43033$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,041$; $p=0,356$). Yani bu hipotez reddedilmiştir.

H_{12.3}: “Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Personelin Nitelięi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından personelin nitelięi ile ilgili ifadelerle ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.59: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Personelin Nitelięi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	4,1458±,64816	0,096	,908
	<i>Yüksek Lisans</i>	4,1509±,53785		
	<i>Doktora</i>	4,2500±,59512		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1458$, $S=0,64816$), yüksek lisans mezunları ($\bar{x}=4,1509$, $S=0,53785$), doktora mezunları ($\bar{x}=4,2500$, $S=0,59512$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,096$; $p=0,908$). Yani bu hipotez reddedilmiştir.

H_{12.4}: “Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBS değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri raporu ile ilgili ifadelerle ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.60: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	3,9611±,74685	0,066	,936
	<i>Yüksek Lisans</i>	3,9245±,56855		
	<i>Doktora</i>	4,0000±,54433		

Analiz sonucunda lisans mezunları ($\bar{x}=3,9611$, $S=0,74685$), yüksek lisans mezunları ($\bar{x}=3,9245$, $S=0,56855$), doktora mezunları ($\bar{x}=4,0000$, $S=0,54433$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,066$; $p=0,936$). Yani bu hipotez reddedilmiştir.

H_{12.5}: “Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBS değerlendirme sınıflarından erişim güvenliği raporu ile ilgili ifadelerle ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.61: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	3,9389±,66805	0,277	,758
	<i>Yüksek Lisans</i>	3,8868±,62683		
	<i>Doktora</i>	3,7619±,53452		

Analiz sonucunda lisans mezunları ($\bar{x}=3,9389$, $S=0,66805$), yüksek lisans mezunları ($\bar{x}=3,8868$, $S=0,62683$), doktora mezunları ($\bar{x}=3,7619$, $S=0,53452$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,277$; $p=0,758$). Yani bu hipotez reddedilmiştir.

H_{12.6}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.62: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	4,1111±,74578	0,514	,599
	<i>Yüksek Lisans</i>	4,0063±,63881		
	<i>Doktora</i>	4,2381±,85449		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1111$, $S=0,74578$), yüksek lisans mezunları ($\bar{x}=4,0063$, $S=0,63881$), doktora mezunları ($\bar{x}=4,2381$, $S=0,85449$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,514$ $p=0,599$). Yani bu hipotez reddedilmiştir.

H_{12.7}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.63: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	4,1667±,61830	1,745	,179
	<i>Yüksek Lisans</i>	3,9560±,67948		
	<i>Doktora</i>	4,2381±,53452		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1667$, $S=0,61830$), yüksek lisans mezunları ($\bar{x}=3,9560$, $S=0,67948$), doktora mezunları ($\bar{x}=4,2381$, $S=0,53452$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,745$ $p=0,179$). Yani bu hipotez reddedilmiştir.

H_{12.8}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin görüşlerinin eğitim durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.64: Eğitim Durumuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Eğitim Durumu	<i>Lisans</i>	4,2444±,70475	0,986	,376
	<i>Yüksek Lisans</i>	4,0818±,67275		
	<i>Doktora</i>	4,3333±,57735		

Analiz sonucunda lisans mezunları ($\bar{x}=4,2444$, $S=0,70475$), yüksek lisans mezunları ($\bar{x}=4,0818$, $S=0,67275$), doktora mezunları ($\bar{x}=4,3333$, $S=0,57735$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,986$ $p=0,376$). Yani bu hipotez reddedilmiştir.

H_{12.9}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Eğitim Durumuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından dıř hizmet saęlayıcılarının yönetimi ile ilgili ifadelere ilişkin görüřlerinin eęitim durumuna göre anlamlı bir farklılık gösterip göstermedięini belirlemek için tek yönlü varyans analizi yapılmıřtır.

Tablo 3.65: Eęitim Durumuna Göre Baęımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Dıř Hizmet Saęlayıcılarının Yönetimi ile İlgili İfadelere İliřkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P deęeri</i>
Eęitim Durumu	<i>Lisans</i>	4,1889±,57364	1,322	,271
	<i>Yüksek Lisans</i>	4,0126±,57350		
	<i>Doktora</i>	4,0476±,73102		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1889$, $S=0,57364$), yüksek lisans mezunları ($\bar{x}=4,0126$, $S=0,57350$), doktora mezunları ($\bar{x}=4,0476$, $S=0,73102$) arasında istatistiksel olarak anlamlı bir fark bulunmamıřtır ($F=1,322$ $p=0,271$). Yani bu hipotez reddedilmiřtir.

H_{12.10}: “Baęımsız Denetçilerin ÖEBSĐ Deęerlendirme Sınıflarından Hizmet Yazılımlarına İliřkin Kontroller ile İlgili İfadelere İliřkin Bilgi Düzeyleri Eęitim Durumuna Göre Farklılařmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelere ilişkin görüřlerinin eęitim durumuna göre anlamlı bir farklılık gösterip göstermedięini belirlemek için tek yönlü varyans analizi yapılmıřtır.

Tablo 3.66: Eęitim Durumuna Göre Baęımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Hizmet Yazılımlarına İliřkin Kontroller ile İlgili İfadelere İliřkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P deęeri</i>
Eęitim Durumu	<i>Lisans</i>	4,1083± ,66122	,317	,729
	<i>Yüksek Lisans</i>	4,1415± ,44265		
	<i>Doktora</i>	4,2857± ,50885		

Analiz sonucunda lisans mezunları ($\bar{x}=4,1083$, $S=0,66122$), yüksek lisans mezunları ($\bar{x}=4,1415$, $S=0,44265$), doktora mezunları ($\bar{x}=4,2857$, $S=0,50885$) arasında

istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,317$ $p=0,729$). Yani bu hipotez reddedilmiştir.

H₁₃: “Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi sonuçları aşağıda yer almaktadır.

Tablo 3.67: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Bağımsız denetçi olarak çalışma süresi	<i>1-5 yıl</i>	3,9321±,45652	4,870	,003
	<i>6-10 yıl</i>	4,1156±,43823		
	<i>11-15 yıl</i>	4,2513±,47446		
	<i>16 yıl ve üzeri</i>	4,3174±,38793		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=3,9321$, $S=0,45652$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,1156$ $S=0,43823$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,2513$, $S=0,47446$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,3174$, $S=0,47446$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=4,870$; $p=0,003$).

Tablo 3.68: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>1-5 yıl</i>	<i>6-10 yıl</i>	<i>11-15 yıl</i>	<i>16 yıl ve üzeri</i>	<i>1-5 yıl</i>
<i>1-5 yıl</i>		,255	,097	,004	
<i>6-10 yıl</i>	,255		,786	,343	,255
<i>11-15 yıl</i>	,097	,786		,973	,097
<i>16 yıl ve üzeri</i>	,004	,343	,973		,004

Çalışma süresi için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden

Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=3,9321$, $S=0,45652$) ile 16 yıl ve üzeri ($\bar{x}=4,3174$, $S=0,47446$) arasında olduğu görülmüştür ($p=0,003$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,004$). Bu sonuca göre “*Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Farklılaşmaktadır*” hipotezi kabul edilmiştir.

H_{13.1}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin, katılımcıların bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.69: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	4,0481±,42020	3,340	,022
	<i>6-10 yıl</i>	4,1406±,51563		
	<i>11-15 yıl</i>	4,3077±,48038		
	<i>16 yıl ve üzeri</i>	4,3804±,41880		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=4,0481$, $S=0,42020$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,1406$, $S=0,51563$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,3077$, $S=0,48038$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,3804$, $S=0,41880$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=3,340$; $p=0,022$). Hipotez kabul edilmiştir.

Tablo 3.70: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	1-5 yıl	6-10 yıl	11-15 yıl	16 yıl ve üzeri
1-5 yıl		,801	,258	,021
6-10 yıl	,801		,678	,220
11-15 yıl	,258	,678		,967
16 yıl ve üzeri	,021	,220	,967	

Çalışma süresi için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=4,0481$, $S=0,42020$) ile 16 yıl ve üzeri ($\bar{x}=4,3804$, $S=0,41880$) arasında olduğu görülmüştür ($p=0,022$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,021$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporunun*” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

H_{13.2}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.71: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,8846±,66629	5,797	,001
	<i>6-10 yıl</i>	4,0833±,52192		
	<i>11-15 yıl</i>	4,3333±,65263		
	<i>16 yıl ve üzeri</i>	4,4783±,54888		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=3,8846$, $S=0,66629$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,0833$ $S=0,52192$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,3333$, $S=0,65263$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,4783$, $S=0,54888$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=5,797$; $p=0,001$). Hipotez kabul edilmiştir.

Tablo 3.72: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>1-5 yıl</i>	<i>6-10 yıl</i>	<i>11-15 yıl</i>	<i>16 yıl ve üzeri</i>
<i>1-5 yıl</i>		,468	,086	,001
<i>6-10 yıl</i>	,468		,596	,087
<i>11-15 yıl</i>	,086	,596		,902
<i>16 yıl ve üzeri</i>	,001	,087	,902	

Çalışma süresi için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın 1-5 yıl($\bar{x}=3,8846$, $S=0,66629$) ile 16 yıl ve üzeri ($\bar{x}=4,4783$, $S=0,54888$) arasında olduğu görülmüştür ($p=0,001$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,001$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “ÖEBS değerlendirme sınıflarından iç kontrol ve denetim mekanizmalarının” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

H_{13.3}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği raporu ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.73: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	4,0192±,54198	2,819	,042
	<i>6-10 yıl</i>	4,1953±,61806		
	<i>11-15 yıl</i>	4,0962±,80064		
	<i>16 yıl ve üzeri</i>	4,4348±,45985		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=4,0192$, $S=0,54198$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,1953$ $S=0,61806$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,0962$, $S=0,80064$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,4348$, $S=0,45985$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=2,819$; $p=0,042$). Hipotez kabul edilmiştir.

Tablo 3.74: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>1-5 yıl</i>	<i>6-10 yıl</i>	<i>11-15 yıl</i>	<i>16 yıl ve üzeri</i>
<i>1-5 yıl</i>		,534	,974	,026
<i>6-10 yıl</i>	,534		,954	,436
<i>11-15 yıl</i>	,974	,954		,339
<i>16 yıl ve üzeri</i>	,026	,436	,339	

Çalışma süresi için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=4,0192$, $S=0,54198$) ile 16 yıl ve üzeri ($\bar{x}=4,4348$, $S=0,45985$) arasında olduğu

görülmüştür ($p=0,042$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,026$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “ÖEBSD değerlendirme sınıflarından personelin niteliğinin” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler.

H_{13.4}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.75: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,8205±,58097	2,231	,088
	<i>6-10 yıl</i>	3,8958±,74985		
	<i>11-15 yıl</i>	4,1538±,77717		
	<i>16 yıl ve üzeri</i>	4,1884±,55801		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=3,8205$, $S=0,58097$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=3,8958$ $S=0,74985$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,1538$, $S=0,77717$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,1884$, $S=0,55801$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=2,231$; $p=0,088$). Yani bu hipotez reddedilmiştir.

H_{13.5}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.76: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Erişim Güvenliği ile İlgili İfadelerle İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,8205±,66490	1,936	,128
	<i>6-10 yıl</i>	3,8125±,59831		
	<i>11-15 yıl</i>	4,0256±,58471		
	<i>16 yıl ve üzeri</i>	4,1594±,62660		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=3,8205$, $S=0,66490$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=3,8125$ $S=0,59831$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,0256$, $S=0,58471$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,1594$, $S=0,62660$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,936$; $p=0,128$). Yani bu hipotez reddedilmiştir.

H_{13.6}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelerle İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.77: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelerle İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,8526±,70607	3,208	,026
	<i>6-10 yıl</i>	4,2188±,64818		
	<i>11-15 yıl</i>	4,2051±,86644		
	<i>16 yıl ve üzeri</i>	4,2899±,56232		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=3,8526$, $S=0,70607$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,2188$ $S=0,64818$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,2051$, $S=0,86644$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,2899$, $S=0,56232$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=3,208$; $p=0,026$). Hipotez kabul edilmiştir.

Tablo 3.78: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	1-5 yıl	6-10 yıl	11-15 yıl	16 yıl ve üzeri
1-5 yıl		,087	,350	,048
6-10 yıl	,087		1,000	,981
11-15 yıl	,350	1,000		,984
16 yıl ve üzeri	,048	,981	,984	

Çalışma süresi için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=3,8526$, $S=0,70607$) ile 16 yıl ve üzeri ($\bar{x}=4,2899$, $S=0,56232$) arasında olduğu görülmüştür ($p=0,026$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,048$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planlarının*” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

H_{13.7}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelerle İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre

anlamli bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.79: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	4,0321±,68044	0,617	,605
	<i>6-10 yıl</i>	4,0208±,64446		
	<i>11-15 yıl</i>	4,2564±,65481		
	<i>16 yıl ve üzeri</i>	4,1594±,57621		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=4,0321$, $S=0,68044$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,0208$ $S=0,64446$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,2564$, $S=0,65448$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,1594$, $S=0,57621$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=0,617$; $p=0,605$). Yani bu hipotez reddedilmiştir.

H_{13.8}: “Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBS D değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.80: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Değişiklik Yönetimi Raporu ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	4,1346±,61307	1,375	,254
	<i>6-10 yıl</i>	4,0417±,79312		
	<i>11-15 yıl</i>	4,3333±,75768		
	<i>16 yıl ve üzeri</i>	4,3768±,61385		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=4,1346$, $S=0,61307$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,0417$ $S=0,79312$), çalışma süresi 11-15 yıl arası

olanlar ($\bar{x}=4,3333$, $S=0,75768$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,3768$, $S=0,61385$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,375$; $p=0,254$). Yani bu hipotez reddedilmiştir.

H_{13.9}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.81: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,9295±,59532	2,877	,039
	<i>6-10 yıl</i>	4,2188±,55267		
	<i>11-15 yıl</i>	4,2051±,75202		
	<i>16 yıl ve üzeri</i>	4,2754±,39762		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=3,9295$, $S=0,59532$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,2188$, $S=0,55267$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,2051$, $S=0,75202$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,2754$, $S=0,39762$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=2,877$; $p=0,039$). Hipotez kabul edilmiştir.

Tablo 3.82: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>1-5 yıl</i>	<i>6-10 yıl</i>	<i>11-15 yıl</i>	<i>16 yıl ve üzeri</i>
<i>1-5 yıl</i>		,115	,407	,048
<i>6-10 yıl</i>	,115		1,000	,984
<i>11-15 yıl</i>	,407	1,000		,985
<i>16 yıl ve üzeri</i>	,048	,984	,985	

Çalışma süresi için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=3,9295$, $S=0,59532$) ile 16 yıl ve üzeri ($\bar{x}=4,2754$, $S=0,39762$) arasında olduğu görülmüştür ($p=0,039$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,048$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetiminin” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

H_{13.10}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.83: Bağımsız Denetçi Olarak Çalışma Süresine Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Bağımsız Denetçi Olarak Çalışma Süresi	<i>1-5 yıl</i>	3,9327± ,48283	4,600	,004
	<i>6-10 yıl</i>	4,2500± ,58199		
	<i>11-15 yıl</i>	4,2115± ,74194		
	<i>16 yıl ve üzeri</i>	4,3804± ,46386		

Analiz sonucunda çalışma süresi 1-5 yıl arası olanlar ($\bar{x}=3,9327$, $S=0,48283$), çalışma süresi 6-10 yıl arası olanlar ($\bar{x}=4,2500$ $S=0,58199$), çalışma süresi 11-15 yıl arası olanlar ($\bar{x}=4,2115$, $S=0,74194$), çalışma süresi 16 yıl ve üzeri olanlar ($\bar{x}=4,3804$,

S=0,46386) arasında istatistiksel olarak anlamlı bir fark bulunmuştur (F=4,600; p=0,004). Hipotez kabul edilmiştir.

Tablo 3.84: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	1-5 yıl	6-10 yıl	11-15 yıl	16 yıl ve üzeri
1-5 yıl		,048	,345	,007
6-10 yıl	,048		,996	,813
11-15 yıl	,345	,996		,803
16 yıl ve üzeri	,007	,813	,803	

Çalışma süresi için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın hem 1-5 yıl ($\bar{x}=3,9327$, S=0,48283) ile 6-10 yıl ($\bar{x}=4,2500$, S=0,58199) arasında olduğu hemde 1-5 yıl ($\bar{x}=3,9327$, S=0,48283) ile 16 yıl ve üzeri ($\bar{x}=4,3804$, S=0,46386) arasında olduğu görülmüştür (p=0,004). Yapılan bu testin sonucunda çalışma süresi 6-10 yıl grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur (p=0,048). Ayrıca yapılan bu testin diğer sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur (p=0,007). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre ve 6-10 yıl tecrübeye sahip denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetiminin” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur (p>0,05).

H₁₄: “Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin bağımsız denetçi olarak denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla yapılan tek yönlü varyans analizi sonuçları aşağıda yer almaktadır.

Tablo 3.85: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine Ait Görüşlerine İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,9575±,40998	2,995	,022
	<i>Denetçi</i>	4,0613±,47626		
	<i>Kıdemli Denetçi</i>	4,0483±,38044		
	<i>Baş Denetçi</i>	4,4176±,36307		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0961±,57601		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=3,9575$, $S=0,40998$), denetçi olanlar ($\bar{x}=4,0613$, $S=0,47626$), kıdemli denetçi olanlar ($\bar{x}=4,0483$, $S=0,38044$), baş denetçi olanlar ($\bar{x}=4,4176$, $S=0,36307$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,0961$, $S=0,57601$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=2,995$; $p=0,022$). “Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Farklılaşmaktadır” hipotezi kabul edilmiştir.

Tablo 3.86: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>Denetçi Yardımcısı</i>	<i>Denetçi</i>	<i>Kıdemli Denetçi</i>	<i>Baş Denetçi</i>	<i>Sorumlu Ortak Baş Denetçi</i>
<i>Denetçi Yardımcısı</i>		,883	,956	,009	,849
<i>Denetçi</i>	,883		1,000	,057	,999
<i>Kıdemli Denetçi</i>	,956	1,000		,097	,998
<i>Baş Denetçi</i>	,009	,057	,097		,230
<i>Sorumlu Ortak Baş Denetçi</i>	,849	,999	,998	,230	

Denetim firmasındaki pozisyonu için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın denetçi yardımcısı ($\bar{x}=3,9575$, $S=0,40998$) ile baş denetçi ($\bar{x}=4,4176$, $S=0,36307$) arasında olduğu görülmüştür ($p=0,009$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,001$). Bu sonuca göre “Denetim Firmasındaki Pozisyonuna Göre

Bağımsız Denetçilerin, E-Belge Özel Entegratörleri Bilgi Sistem Denetimine İlişkin Bilgi Düzeyleri Farklaşmaktadır” hipotezi kabul edilmiştir.

H_{14.1}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.87: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	4,0776±,33477	1,554	,191
	<i>Denetçi</i>	4,1622±,55969		
	<i>Kıdemli Denetçi</i>	4,1125±,44776		
	<i>Baş Denetçi</i>	4,4118±,38468		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,1324±,50092		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=4,0776$, $S=0,33477$), denetçi olanlar ($\bar{x}=4,1622$, $S=0,55969$), kıdemli denetçi olanlar ($\bar{x}=4,1125$, $S=0,44776$), baş denetçi olanlar ($\bar{x}=4,4118$, $S=0,38468$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,1324$, $S=0,50092$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,554$; $p=0,191$). Bu hipotez reddedilmiştir.

H_{14.2}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından İç Kontrol ve Denetim Mekanizmaları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerine ilişkin görüşlerinin denetim firmasındaki pozisyonuna

göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.88: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBS D Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelerine İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,7931±,68669	5,162	,001
	<i>Denetçi</i>	4,0811±,56331		
	<i>Kıdemli Denetçi</i>	4,1333±,50029		
	<i>Baş Denetçi</i>	4,6275±,38877		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0980±,78850		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=3,7931$, $S=0,68669$), denetçi olanlar ($\bar{x}=4,0811$, $S=0,56331$), kıdemli denetçi olanlar ($\bar{x}=4,1333$, $S=0,50029$), baş denetçi olanlar ($\bar{x}=4,6275$, $S=0,38887$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,0980$, $S=0,78850$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=5,162$; $p=0,001$). Hipotez kabul edilmiştir.

Tablo 3.89: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>Denetçi Yardımcısı</i>	<i>Denetçi</i>	<i>Kıdemli Denetçi</i>	<i>Baş Denetçi</i>	<i>Sorumlu Ortak Baş Denetçi</i>
<i>Denetçi Yardımcısı</i>		,309	,301	,001	,465
<i>Denetçi</i>	,309		,998	,020	1,000
<i>Kıdemli Denetçi</i>	,301	,998		,101	1,000
<i>Baş Denetçi</i>	,001	,020	,101		,084
<i>Sorumlu Ortak Baş Denetçi</i>	,465	1,000	1,000	,084	

Denetim firmasındaki pozisyonu için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın hem denetçi yardımcısı ($\bar{x}=3,7931$, $S=0,68669$) ile baş denetçi ($\bar{x}=4,6275$, $S=0,38887$) arasında hemde denetçi ($\bar{x}=4,0811$, $S=0,56331$) ile baş denetçi ($\bar{x}=4,6275$, $S=0,38887$) arasında olduğu görülmüştür ($p=0,001$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,001$). Ayrıca denetim firmasındaki çalışma pozisyonu baş denetçi olan

grubun ortalaması, denetçi olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,02$). Bu sonuca göre baş denetçilerin “*ÖEBSD Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadeler*” denetçi yardımcılara ve denetçilere göre daha fazla katıldıkları görülmektedir. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

H_{14.3}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin Niteliği ile İlgili İfadelerle İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.90: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Personelin ile İlgili İfadelerle İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	4,0000±,46291	2,343	,059
	<i>Denetçi</i>	4,2432±,63598		
	<i>Kıdemli Denetçi</i>	4,0500±,62618		
	<i>Baş Denetçi</i>	4,4706±,58552		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0294±,57881		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=4,0000$, $S=0,46291$), denetçi olanlar ($\bar{x}=4,2432$, $S=0,63598$), kıdemli denetçi olanlar ($\bar{x}=4,0500$, $S=0,62618$), baş denetçi olanlar ($\bar{x}=4,4706$ $S=0,58552$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,0294$, $S=0,57881$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=2,343$; $p=0,059$). Hipotez reddedilmiştir.

H_{14.4}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelerle İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelere iliřkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.91: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Fiziki Şartlar ve Güvenlik Tedbirleri ile İlgili İfadelere İliřkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P deęeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,8966±,59830	2,264	,067
	<i>Denetçi</i>	3,7387±,74592		
	<i>Kıdemli Denetçi</i>	4,0000±,61178		
	<i>Baş Denetçi</i>	4,2353±,56230		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,1373±,58995		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=3,8966$, $S=0,59830$), denetçi olanlar ($\bar{x}=3,7387$, $S=0,74592$), kıdemli denetçi olanlar ($\bar{x}=4,0000$, $S=0,61178$), baş denetçi olanlar ($\bar{x}=4,2353$, $S=0,56230$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,1373$, $S=0,58995$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=2,264$; $p=0,067$). Hipotez reddedilmiştir.

H_{14.5}: “Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Eriřim Güvenlięi ile İlgili İfadelere İliřkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından erişim güvenliği ile ilgili ifadelere iliřkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.92: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Deęerlendirme Sınıflarından Eriřim Güvenlięi ile İlgili İfadelere İliřkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P deęeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,9310±,63233	2,340	,059
	<i>Denetçi</i>	3,7117±,57822		
	<i>Kıdemli Denetçi</i>	3,8333±,56713		
	<i>Baş Denetçi</i>	4,2353±,65367		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0392±,74426		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=3,9310$, $S=0,63233$), denetçi olanlar ($\bar{x}=3,7117$, $S=0,57822$), kıdemli denetçi olanlar ($\bar{x}=3,8333$, $S=0,56713$), baş denetçi olanlar ($\bar{x}=4,2353$, $S=0,65367$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,0392$, $S=0,74426$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=2,340$; $p=0,059$). Hipotez reddedilmiştir.

H_{14.6}: “Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBS değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.93: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBS Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	P değeri
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,8506±,64603	2,794	,029
	<i>Denetçi</i>	4,1892±,66916		
	<i>Kıdemli Denetçi</i>	3,9500±,74359		
	<i>Baş Denetçi</i>	4,4706±,51450		
	<i>Sorumlu Ortak Baş Denetçi</i>	3,9412±,83529		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=3,8506$, $S=0,64603$), denetçi olanlar ($\bar{x}=4,1892$, $S=0,6916$), kıdemli denetçi olanlar ($\bar{x}=3,9500$, $S=0,74359$), baş denetçi olanlar ($\bar{x}=4,4706$, $S=0,51450$), sorumlu ortak baş denetçi olanlar ($\bar{x}=3,9412$, $S=0,83529$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=2,794$; $p=0,029$). Hipotez kabul edilmiştir.

Tablo 3.94: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>Denetçi Yardımcısı</i>	<i>Denetçi</i>	<i>Kıdemli Denetçi</i>	<i>Baş Denetçi</i>	<i>Sorumlu Ortak Baş Denetçi</i>
<i>Denetçi Yardımcısı</i>		,274	,987	,029	,993
<i>Denetçi</i>	,274		,715	,626	,729
<i>Kıdemli Denetçi</i>	,987	,715		,149	1,000
<i>Baş Denetçi</i>	,029	,626	,149		,166
<i>Sorumlu Ortak Baş Denetçi</i>	,993	,729	1,000	,166	

Denetim firmasındaki pozisyonu için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın denetçi yardımcısı ($\bar{x}=3,8506$, $S=0,64603$) ile baş denetçi ($\bar{x}=4,4706$, $S=0,51450$) arasında olduğu görülmüştür ($p=0,029$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,029$). Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$). Bu sonuca göre baş denetçilerin “*ÖEBSD Değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere*” denetçi yardımcılarına göre daha fazla katıldıkları görülmektedir.

H_{14.7}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.95: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	4,0230±,57688	2,544	,043
	<i>Denetçi</i>	4,1712±,62173		
	<i>Kıdemli Denetçi</i>	3,7500±,79380		
	<i>Baş Denetçi</i>	4,3725±,52549		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0588±,61503		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=4,0230$, $S=0,57688$), denetçi olanlar ($\bar{x}=4,1712$, $S=0,62173$), kıdemli denetçi olanlar ($\bar{x}=3,5500$, $S=0,79380$), baş denetçi olanlar ($\bar{x}=4,3725$, $S=0,52549$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,0588$, $S=0,61503$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=2,544$; $p=0,043$). Hipotez kabul edilmiştir.

Tablo 3.96: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>Denetçi Yardımcısı</i>	<i>Denetçi</i>	<i>Kıdemli Denetçi</i>	<i>Baş Denetçi</i>	<i>Sorumlu Ortak Baş Denetçi</i>
<i>Denetçi Yardımcısı</i>		,877	,571	,370	1,000
<i>Denetçi</i>	,877		,121	,811	,974
<i>Kıdemli Denetçi</i>	,571	,121		,027	,574
<i>Baş Denetçi</i>	,370	,811	,027		,596
<i>Sorumlu Ortak Baş Denetçi</i>	1,000	,974	,574	,596	

Denetim firmasındaki pozisyonu için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın kıdemli denetçi ($\bar{x}=3,5500$, $S=0,79380$) ile baş denetçi ($\bar{x}=4,3725$, $S=0,52549$) arasında olduğu görülmüştür ($p=0,043$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, kıdemli denetçi olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,027$). Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$). Bu sonuca göre baş denetçilerin “*ÖEBSD Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadeler*” kıdemli denetçilere göre daha fazla katıldıkları görülmektedir.

H_{14.8}: “Bağımsız Denetçilerin, ÖEBSD Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelerle İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.97: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Değişiklik Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	4,2069±,40251	1,685	,158
	<i>Denetçi</i>	4,0901±,80373		
	<i>Kıdemli Denetçi</i>	4,0500±,80405		
	<i>Baş Denetçi</i>	4,5490±,49918		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,0980±,73376		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=4,2069$, $S=0,40251$), denetçi olanlar ($\bar{x}=4,0901$, $S=0,80373$), kıdemli denetçi olanlar ($\bar{x}=4,0500$, $S=0,80405$), baş denetçi olanlar ($\bar{x}=4,5490$ $S=0,49918$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,0980$, $S=0,73376$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,685$; $p=0,158$). Bu hipotez reddedilmiştir.

H_{14.9}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.98: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Dış Hizmet Sağlayıcılarının Yönetimi ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	4,0345±,49075	1,042	,389
	<i>Denetçi</i>	4,0901±,62681		
	<i>Kıdemli Denetçi</i>	4,0000±,74927		
	<i>Baş Denetçi</i>	4,3529±,44831		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,1176±,52627		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=4,0345$, $S=0,49075$), denetçi olanlar ($\bar{x}=4,0901$, $S=0,62681$), kıdemli denetçi olanlar

($\bar{x}=4,0000$, $S=0,74927$), baş denetçi olanlar ($\bar{x}=4,3529$ $S=0,44831$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,1176$, $S=0,52627$) arasında istatistiksel olarak anlamlı bir fark bulunmamıştır ($F=1,042$; $p=0,389$).Bu hipotez reddedilmiştir.

H_{14.10}: “Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere İlişkin Bilgi Düzeyleri Denetim Firmasındaki Pozisyonuna Göre Farklılaşmaktadır.”

Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek için tek yönlü varyans analizi yapılmıştır.

Tablo 3.99: Denetim Firmasındaki Pozisyonuna Göre Bağımsız Denetçilerin, ÖEBSĐ Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere İlişkin Tek Yönlü Varyans Analizi Sonuçları

<i>Tek Yönlü Varyans Analizi</i>		$\bar{x} \pm S$	F	<i>P değeri</i>
Denetim Firmasındaki Pozisyonu	<i>Denetçi Yardımcısı</i>	3,9310± ,42729	2,861	,027
	<i>Denetçi</i>	4,0608± ,64390		
	<i>Kıdemli Denetçi</i>	4,2000± ,48395		
	<i>Baş Denetçi</i>	4,4559± ,42606		
	<i>Sorumlu Ortak Baş Denetçi</i>	4,2353± ,65830		

Analiz sonucunda denetim firmasındaki pozisyonu denetçi yardımcısı olanlar ($\bar{x}=3,9310$, $S=0,42729$), denetçi olanlar ($\bar{x}=4,0608$, $S=0,64390$), kıdemli denetçi olanlar ($\bar{x}=4,2000$, $S=0,48395$), baş denetçi olanlar ($\bar{x}=4,4559$, $S=0,42606$), sorumlu ortak baş denetçi olanlar ($\bar{x}=4,2353$, $S=0,65830$) arasında istatistiksel olarak anlamlı bir fark bulunmuştur ($F=2,861$; $p=0,027$). Hipotez kabul edilmiştir.

Tablo 3.100: Tukey in HSD Test Sonuçları

POST HOC Tukey HSD	<i>Denetçi Yardımcısı</i>	<i>Denetçi</i>	<i>Kıdemli Denetçi</i>	<i>Baş Denetçi</i>	<i>Sorumlu Ortak Baş Denetçi</i>
<i>Denetçi Yardımcısı</i>		,873	,442	,018	,365
<i>Denetçi</i>	,873		,889	,105	,811
<i>Kıdemli Denetçi</i>	,442	,889		,616	1,000
<i>Baş Denetçi</i>	,018	,105	,616		,764
<i>Sorumlu Ortak Baş Denetçi</i>	,365	,811	1,000	,764	

Denetim firmasındaki pozisyonu için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır. Yapılan analiz sonucunda anlamlı farklılığın denetçi yardımcısı ($\bar{x}=3,9310$, $S=0,42729$) ile baş denetçi ($\bar{x}=4,4559$, $S=0,42606$) arasında olduğu görülmüştür ($p=0,027$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,018$). Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$). Bu sonuca göre baş denetçilerin “*ÖEBSD Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadelere*” denetçi yardımcılarında göre daha fazla katıldıkları görülmektedir.

Yapılan çalışmada test edilen hipotezlere ait sonuçlar Tablo 3.101’de verilmiştir.

Tablo 3.101: Araştırma Hipotezlerinin Sonuçları

	Hipotezler	Sonuç
H ₁	Bilgi sistem denetimi ile bağımsız denetim arasında anlamlı bir ilişki vardır.	KABUL
H ₂	Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri cinsiyetlerine göre farklılaşmaktadır.	RED
H ₃	Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED
H ₄	Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri yaş durumuna göre farklılaşmaktadır.	RED
H ₅	Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri eğitim durumuna göre farklılaşmaktadır.	RED
H ₆	Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	RED

H7	Bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	KABUL
H8	Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri yüksektir.	KABUL
H9	Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H9.1	Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H9.2	Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H9.3	Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H9.4	Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H9.5	Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H9.6	Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H9.7	Bağımsız denetçilerin, ÖEBSĐ değerlendirme sınıflarından denetim izleri yönetimi raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED

H_{9.8}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H_{9.9}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H_{9.10}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır.	RED
H₁₀	Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	KABUL
H_{10.1}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED
H_{10.2}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	KABUL
H_{10.3}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED
H_{10.4}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	KABUL
H_{10.5}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından erişim güvenliği raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED

H_{10.6}	Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iş süreklilięi, risk yönetimi ve acil durum planları raporu ile ilgili ifadelerle ilişkin ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED
H_{10.7}	Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından denetim izleri yönetimi raporu ile ilgili ifadelerle ilişkin ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED
H_{10.8}	Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından deęişiklik yönetimi raporu ile ilgili ifadelerle ilişkin ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED
H_{10.9}	Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi raporu ile ilgili ifadelerle ilişkin ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	RED
H_{10.10}	Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller raporu ile ilgili ifadelerle ilişkin ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.	KABUL
H₁₁	Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H_{11.1}	Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H_{11.2}	Bağımsız denetçilerin, ÖEBSĐ deęerlendirme sınıflarından iç kontrol ve denetim mekanizmaları raporu ile ilgili ifadelerle ilişkin ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED

H11.3	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H11.4	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H11.5	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelerle ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H11.6	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H11.7	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H11.8	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H11.9	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H11.10	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller raporu ile ilgili ifadelerle ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır.	RED
H12	Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H12.1	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED

H _{12.2}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.3}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.4}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.5}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.6}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.7}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.8}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.9}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H _{12.10}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır.	RED
H ₁₃	Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	KABUL
H _{13.1}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile	KABUL

	ilgili ifadelerine ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	
H13.2	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelere ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	KABUL
H13.3	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelere ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	KABUL
H13.4	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	RED
H13.5	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelere ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	RED
H13.6	Bağımsız denetçilerin, ÖEBSD değerlendirme Sınıflarından İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları ile İlgili İfadelere İlişkin Bilgi Düzeyleri Bağımsız Denetçi Olarak Çalışma Süresine Göre Farklılaşmaktadır.	KABUL
H13.7	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelere ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	RED
H13.8	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi raporu ile ilgili ifadelere ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	RED
H13.9	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelere ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	KABUL
H13.10	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelere ilişkin bilgi	KABUL

	düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır.	
H₁₄	Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	KABUL
H_{14.1}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	RED
H_{14.2}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	RED
H_{14.3}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	RED
H_{14.4}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından fiziki şartlar ve güvenlik tedbirleri ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	RED
H_{14.5}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından erişim güvenliği ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	RED
H_{14.6}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	KABUL
H_{14.7}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	KABUL
H_{14.8}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından değişiklik yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	RED

H_{14.9}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	RED
H_{14.10}	Bağımsız denetçilerin, ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır.	KABUL



SONUÇ VE ÖNERİLER

Küreselleşen dünyada yaşanan teknolojik gelişmeler, hemen hemen her alanda iş kolunu ve meslekleri etkisi altına alarak çağın ihtiyaçlarına göre kendilerini yenilemelerini gerekli hale getirmiştir. İşletmelerin gelişen rekabet ortamında başarı sağlayabilmeleri için bu gelişmeleri takip etmeleri gerekir. Hızlı ve doğru bilgiye ulaşmanın çok önemli olduğu muhasebe ve denetim alanlarında da bu değişimlerin yaşanması kaçınılmaz olmuştur.

Bilgi teknolojilerinde yaşanan gelişmelerle birlikte ülkemizde maliyenin elektronik uygulamalarıyla (e-defter, e-fatura v.b) artık bu bilgiler bilgi sistemleri aracılığıyla eş zamanlı olarak bilgi kullanıcılarına iletilebilmektedir. Bu bağlamda çıkarılan yasal düzenlemeler ile bilgi akışı ve raporlama, bilgi sistemleri ortamında olabilmektedir. İşletmelerin muhasebe kayıtlarını e-defter üzerinden tutmaları, beyannamelerini aynı sistem üzerinden vermeleri, işletme ile bilgi kullanıcıları arasındaki bilgi transferlerini oldukça hızlı hale getirmektedir. Bu uygulamalar önemli ölçüde maliyetlerde azalmaya sebep olması, gönderilen ve alınan faturalara anlık ulaşımın sağlanması, vergi kayıplarının ve kaçaklarının önlenmesi, vergi denetiminin daha hızlı yapılabilmesi v.b avantajlar sağlamaktadır.

Finansal bilginin, bilgi sistemleri kapsamında işlenmesi, üretilmesi ve saklanması nedeniyle bağımsız denetim gerçekleştirilirken, elektronikleşen kayıt ortamında oluşabilecek hata ve hilelerin ortaya çıkabileceği bu nedenle sistemlere odaklanması gerektiği kabul gören bir gerçektir. Bu durum bilgi sistemleri denetiminin gerekliliğinin önemini ortaya koymuştur. Bu kapsamda dünyada ve ülkemizde de bilgi sistemleri denetimini gerekliliğine yönelik birtakım düzenlemeler gerçekleşmiştir. Ülkemizde Sayıştay tarafından 2013 yılının haziran ayında “*Bilgi Sistemleri Denetim Rehberi*” yayımlanmıştır. Bankaların kullandıkları bilgi sistemlerinin yönetimi ile ilgili pek çok yayımlanan tebliğ ve yönetmeliğin (düzenlenmenin) ardından son olarak 31.12.2021 tarihli ve 31706 mükerrer sayılı Resmî Gazete’de “*Bilgi Sistemleri ve İş Süreçleri Bağımsız Denetimine İlişkin Rapor Hakkında Tebliğ*” yayımlanmıştır.

KGK, 660 sayılı Kanun Hükmünde Kararname Madde 9 c bendi “*Finansal tabloların; işletmelerin finansal durumunu, performansını ve nakit akışlarını Türkiye Muhasebe Standartları doğrultusunda gerçeğe uygun olarak sunumunu, kullanıcıların*

ihtiyaçlarına uygunluğunu, güvenilirliğini, şeffaflığını, karşılaştırılabilirliğini ve anlaşılabilirliğini sağlamak amacıyla, kamu yararını da gözetmek suretiyle, bilgi sistemleri denetimi dahil, uluslararası standartlarla uyumlu ulusal denetim standartlarını oluşturmak ve yayımlamak." şeklindedir. 19.11.2019 tarihinde Hazine ve Maliye Bakanlığı-Gelir İdaresi Başkanlığı tarafından “*e-Belge Özel Entegratörleri Bilgi Sistemleri Denetimi Kılavuzu*” yayınlanmıştır. Yayınlanan kılavuzda e-Belge entegratörlerinin faaliyetlerini gerçekleştirmede kullandıkları bilgi sistemlerinin yönetimi ile yetkilendirilmiş bağımsız denetim kuruluşları tarafından denetlenmelerine ilişkin usul ve esasları içeren bilgiler yer almaktadır.

Bu düzenlemelerden anlaşılacağı üzere bilgi sistemleri denetimi bağımsız denetimin bir parçası olup bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekir. Elektronik bilgi sistemlerinin denetim kanıtlarının yapısını değiştirmesi nedeniyle sadece kanıtlara değil kanıtları oluşturan sistemlere de odaklanılması gerekir.

Ülkemizde de dijital dönüşüm kapsamında Maliye Bakanlığına bağlı, Gelir İdaresi Başkanlığı tarafından e-Fatura, e-Arşiv fatura, e-İrsaliye, e-Defter, e-Bilet, e-serbest meslek makbuzu (SMM), e-Müstahsil Makbuzu gibi uygulamaların tamamının e-belge başlığı altında hayata geçtiği görülmektedir. e-Belge; muhasebe alanında kullanılan belgelerin elektronik ortamda oluşturulup ibraz edilmesini sağlayan bir uygulamadır. Pek çok e-belge çeşidi bulunmakta olup hepsinin amacı farklıdır. Bu kapsamda ülkemizde yakından takip edilen ve tüm kamu kurumlarının iş süreçlerine uyarlanan GİB tarafından belirlenen standartlar çerçevesinde elektronik ortamda oluşturulan e-belgelerin bağımsız denetim için kanıt niteliği taşıması nedeniyle çalışmanın konusunu oluşturmaktadır. e-Belgelerin elektronik ortamda iletimi, GİB Web Portal, Doğrudan Entegrasyon veya Özel Entegrasyon ile sağlanabilmektedir. En çok tercih edilen yöntem özel entegrasyon yöntemidir.

Çalışmanın amacı bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşlerini ve e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeylerini araştırmaktır. Bu amaç doğrultusunda Ankara ilinde yer alan bağımsız denetçilere bir anket çalışması yapılmıştır.

Anketin birinci bölümünde bağımsız denetçilerin sosyo-demografik özelliklerinin belirlenmesi amaçlanmıştır. Yapılan araştırma kapsamında ilk olarak katılımcıların

demografik özellikleri incelenmiş olup frekans analizi yapılmış ve elde edilen bulgulara göre katılımcıların 44 (%36,7) 'ü kadın, 76 (%63,3) 'sı erkektir. Çalışmaya katılan bağımsız denetçilerin yaş dağılımlarına göre katılımcıların 21 (%17,5)' inin 30 yaş altında olduğu, 16 (%13,3)' sının 30-39 yaş aralığında olduğu, 42 (%35,0)' sinin 40-49 yaş aralığında olduğu, 24 (%20,0)' ünün 50-59 yaş aralığında olduğu, 17 (%14,2)' sinin 60 yaş üzerinde olduğu, katılımcıların 60 (%50,0)' inin lisans mezunu olduğu, 53 (%44,2)' ünün yüksek lisans mezunu olduğu ve 7 (%5,8)' inin doktora mezunu olduğu görülmektedir.

Katılımcıların 4'ü kadın 13'ü erkek olmak üzere 17 (%14,1)'sinin sorumlu ortak baş denetçi, 7' si kadın 10'u erkek olmak üzere 17 (%14,1)'sinin baş denetçi, 5' i kadın 15'i erkek olmak üzere 20 (%16,7)' sinin kıdemli denetçi, 14' ü kadın 23' ü erkek olmak üzere 37 (%30,9)'sinin denetçi, 14' ü kadın 15' i erkek olmak üzere 29 (%24,2)' unun denetçi yardımcısı unvanına sahip olduğu belirlenmiştir.

Çalışmaya katılan bağımsız denetçilerin çalışma sürelerine ait dağılımlara bakıldığında 1-5 yıl arası çalışma tecrübesi olanlar 52 (%43,3) kişi, 6-10 yıl arası çalışma tecrübesi olanlar 32 (%26,7) kişi, 11-15 yıl arası çalışma tecrübesi olanlar 13 (%10,8) kişi, 16 yıl üzeri çalışma tecrübesi olanlar 23 (%19,2) kişi olarak tespit edilmiştir. Çalışmaya katılan bağımsız denetçilerin %63,3' ünün e-belge özel entegratör kuruluşları hakkında bilgi sahibi oldukları, %13,3'ünün ise bilgi sahibi olmadıkları anlaşılmıştır. Araştırmaya katılan bağımsız denetçilerin %14,2'sinin bilgi sistemleri denetçi sertifikası (CISA)'na sahip oldukları, %85,8'inin ise bu sertifikaya sahip olmadıkları görülmektedir.

Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisine yönelik görüşlerini belirlemek amacıyla hazırlanan ikinci bölümde yer alan sorulara verdikleri yanıtların ortalama ve standart sapma değerlerine bakılmıştır. Bu iki değer birlikte incelendiğinde "Bilgi sistem denetimi ile bağımsız denetim arasında anlamlı bir ilişki vardır" hipotezi kabul edilmiştir.

- Bağımsız Denetçilerin, Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere İlişkin Görüşleri
 - i. Araştırmaya katılan bağımsız denetçilerin "Bilgi sistemleri denetimi bağımsız denetimin bir parçasıdır, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekir." ifadesine %65,8 oranında katıldığı, %20 oranında ise kesinlikle katıldığı görülmektedir. Buna göre, katılımcıların büyük

kısmı (%85,8) bilgi sistemleri denetiminin bağımsız denetimin bir parçası olduğunu bildiklerini, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerektiğini belirtmektedirler.

- ii. “Bağımsız denetimde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeler.” İfadesine katılımcıların %38,3’ü katılıyorum, %43,3’ü kesinlikle katılıyorum, %12,5’i kararsız kalmış, %5,8’i ise katılmamıştır. Buna göre, katılımcıların büyük kısmını (%81,6) bağımsız denetimde bilgi sistemlerinin üzerinde durulmamasının denetimin gerçekleştirilme amacı olan makul güvenceyi zedelediği fikrine sahip olduğu görülmektedir.
- iii. “Bilgi sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkisi vardır.” ifadesine katılımcıların %84,2 oranı ile (%39,2=kesinlikle katılıyorum, %45,0=katılıyorum) büyük çoğunluğunun katıldığı, %15’ininde kararsız olduğu görülmektedir. Buna göre, katılımcılar bilgi sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkiye sahip olduğunu belirtmektedirler.
- iv. Araştırmaya katılan katılımcıların çok büyük bir kısmı (%92,5) “Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.” ifadesine katıldığı görülmektedir. Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışmasının daha şeffaf sonuçların ortaya konmasına katkı sağlayacağı neredeyse tüm katılımcılar tarafından ifade edilmektedir.
- v. “Denetim planı oluşturulurken, denetim riskinin büyüklüğü belirlenirken bilgi sistem denetimi sonuçları dikkate alınmalıdır.” ifadesine bağımsız denetçilerin neredeyse tamamının %93,3’ünün (%55,8= katılıyorum, %37,5=kesinlikle katılıyorum) katıldığı belirlenmiştir. Bu sonuca göre; denetim planı oluşturulurken, denetim riskinin büyüklüğü belirlenirken bilgi sistem denetimi sonuçları dikkate alınmalıdır fikri bağımsız denetçilerin çok büyük bir kısmı tarafından desteklenmektedir.
- vi. Katılımcılara “Bilgi sistemleri denetimin de iç kontrol ve denetim mekanizmaları değerlendirmelerinin bağımsız denetim kanıt güvenilirliğine etkisi vardır.”

ifadesi sunulmuş, %93,4'ü katıldıklarını (%46,7=katılıyorum, %46,7=kesinlikle katılıyorum) belirtmişlerdir.

- vii. Katılımcılara ters bir formatta “Bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki etmez.” ifadesi sunulmuştur. Katılımcıların %77,5'i bu ifadeye katılmadıklarını yani bilgi sistemlerinin söz konusu verileri doğru üretip üretmediğinin bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki edeceğini düşünmektedirler. Bu fikrin tam tersini savunan (%10) kısmında dikkat çekici olduğu ifade edilebilir.
- viii. “Finansal tablolara kaynak verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.” ifadesine katılımcıların büyük çoğunluğunun (%94,1) katıldıkları (%53,3=katılıyorum, %40,8=kesinlikle katılıyorum) görülmektedir.

Sonuç olarak “Bağımsız Denetçilerin Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi ile İlgili İfadelere İlişkin Görüşleri” incelendiğinde ortalamanın $\bar{X}=4,02$ değerini aldığı ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Yani bağımsız denetçilere göre bilgi sistemleri denetiminin bağımsız denetime etkisinin olduğu ve bu etkinin yüksek seviyede olduğu söylenebilir.

Normal dağılıma uyduğu belirlenen gruplar arasındaki anlamlı farklılıkların analizi, iki gruptan oluşanlar için bağımsız örneklem t testi, üç veya daha fazla gruptan oluşanlar için tek yönlü varyans analizi kullanılarak yapılmıştır. Varyans analizinde anlamlı farklılıkların hangi gruplar arasında olduğunu belirlemek için post hoc çoklu karşılaştırmalardan Tukey in HSD testi kullanılmıştır. $p<0,05$ değeri istatistiksel olarak anlamlı kabul edilmiştir.

Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisine ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini görebilmek için cinsiyet gruplarına bağımsız örneklem t-testi gerçekleştirilmiş ve istatistiksel olarak anlamlı bir fark tespit edilmemiştir. Böylece “Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri cinsiyetlerine göre farklılaşmaktadır” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla bağımsız örneklem t Testi yapılmıştır. Analiz sonucunda CISA belgesine sahip olma durumuna göre istatistiksel olarak anlamlı bir fark bulunmamıştır. Dolayısıyla “ Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır ” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin yaş durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda yaş grupları arasında istatistiksel olarak anlamlı bir fark bulunmamıştır. Böylece “Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri yaş durumuna göre farklılaşmaktadır” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin eğitim durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda eğitim durumlarına göre gruplar arasında istatistiksel olarak anlamlı bir fark bulunmamıştır. Bu nedenle “Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri eğitim durumuna göre farklılaşmaktadır” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda bağımsız denetçi olarak çalışma süresine göre gruplar arasında istatistiksel olarak anlamlı bir fark bulunmamıştır. Bu nedenle “Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili görüşleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Denetim firmasındaki pozisyon için yapılan tek yönlü varyans analizinde anlamlı bir farklılık bulunmuştur. Bu nedenle “Bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile

ilgili görüşleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır” hipotezi kabul edilmiştir.

➤ Bağımsız Denetçilerin e- Belge Özel Entegratör Bilgi Sistem Denetimi ile İlgili İfadelere İlişkin Bilgi Düzeyi

Bağımsız denetçilerin e- belge özel entegratör bilgi sistem denetimi ile ilgili ifadelerle ilişkin bilgi düzeylerini belirlemek amacıyla hazırlanan üçüncü bölümde yer alan sorulara verdikleri yanıtların ortalama ve standart sapma değerlerine bakılmıştır. Buna göre ankete katılan “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri” ile ilgili ifadelerle verdiği cevaplar incelendiğinde ortalamanın $\bar{X}=4,0894$ değerini aldığı ve bu ifadenin “katılıyorum” değeri aralığında olduğu belirlenmiştir. Standart sapma değeri ise $SS=0,46236$ olarak bulunmuş ve bu değerin düşük olduğu görülmektedir. Bu iki değer birlikte incelendiğinde “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri yüksektir” hipotezi kabul edilmiştir.

Bağımsız denetçilerin, e- belge özel entegratör bilgi sistem denetimi ile ilgili ifadelerle ilişkin bilgi düzeylerine dair katılımcıların cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini görebilmek için cinsiyet gruplarına bağımsız örneklem t-testi gerçekleştirilmiş ve istatistiksel olarak anlamlı bir fark tespit edilmemiştir. Böylece “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri cinsiyetlerine göre farklılaşmaktadır” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin ISACA tarafından verilen CISA belgesine sahip olma durumuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla bağımsız örneklem t Testi yapılmıştır. Analiz sonucunda CISA belgesine sahip olma durumuna göre istatistiksel olarak anlamlı bir fark bulunmuştur. Dolayısıyla “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri ISACA tarafından verilen CISA belgesine sahip olma durumuna göre farklılaşmaktadır.” hipotezi kabul edilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin yaş durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda yaş grupları arasında istatistiksel olarak anlamlı bir fark bulunmamıştır. Böylece “Bağımsız denetçilerin, e-belge özel

entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri yaş durumuna göre farklılaşmaktadır” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin eğitim durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda eğitim durumlarına göre gruplar arasında istatistiksel olarak anlamlı bir fark bulunmamıştır. Bu nedenle “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri eğitim durumuna göre farklılaşmaktadır” hipotezi reddedilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda bağımsız denetçi olarak çalışma süresine göre gruplar arasında istatistiksel olarak anlamlı bir fark bulunmuştur. Bu nedenle “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri bağımsız denetçi olarak çalışma süresine göre farklılaşmaktadır” hipotezi kabul edilmiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Denetim firmasındaki pozisyon için yapılan tek yönlü varyans analizinde anlamlı bir farklılık bulunmuştur. Bu nedenle “Bağımsız denetçilerin, e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri denetim firmasındaki pozisyonuna göre farklılaşmaktadır” hipotezi kabul edilmiştir.

Bu konuyla ilgili GİB tarafından e-Belge Özel Entegratörleri bilgi sistemleri denetimi klavuzundan faydalanılarak anket soruları 10 ana başlık altında toplanmıştır.

- i. Bağımsız denetçilerin uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporuna ilişkin ifadeler katılma düzeylerinin ortalamasının $\bar{X}=4,16$ olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu görülmektedir. Araştırmaya katılan bağımsız denetçilerin uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporuna ait ifadeler katılma ölçeğinin yüksek seviyede olduğu söylenebilir.

- ii. Bağımsız denetçilerin iç kontrol ve denetim mekanizmalarına ilişkin ifadelerle katılma düzeylerinin ortalamasının $\bar{X}=4,10$ değerinde ve ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu görülmektedir. Araştırmaya katılan bağımsız denetçilerin iç kontrol ve denetim mekanizmalarına ilişkin ifadelerle katılma ölçeğinin yüksek seviyede olduğu söylenebilir.
- iii. Bağımsız denetçilerin personel niteliğine ilişkin ifadelerle katılma düzeylerinin ortalamasının $\bar{X}=4,15$ değerinde olduğu görülmektedir. Bu veriler doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve araştırmaya katılan bağımsız denetçilerin personel niteliğine ilişkin ifadelerle katılma ölçeğinin yüksek seviyede olduğu söylenebilir.
- iv. Bağımsız denetçilerin fiziki şartlar ve güvenlik tedbirlerine ilişkin ifadelerle katılma düzeylerinin ortalamasının $\bar{X}=3,94$ olduğu ve ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu görülmektedir. Araştırmaya katılan bağımsız denetçilerin fiziki şartlar ve güvenlik tedbirlerine ile ilgili fikirlerinin yüksek seviyede olduğu söylenebilir.
- v. Bağımsız denetçilerin erişim güvenliğine ilişkin ifadelerle katılma düzeylerinin ortalamasının $\bar{X}=3,09$ olduğu görülmektedir. Bu veri doğrultusunda, ölçeğin ortalamasının “kararsızım” değer aralığında olduğu ve araştırmaya katılan bağımsız denetçilerin erişim güvenliği ile ilgili fikirlerinin orta seviyede olduğu söylenebilir.
- vi. Bağımsız denetçilerin iş sürekliliği, risk yönetimi ve acil durum planlarına ilişkin ifadelerle katılma düzeylerinin ortalamasının $\bar{X}=3,98$ olduğu görülmektedir. Bu veri doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve araştırmaya katılan bağımsız denetçilerin iş sürekliliği, risk yönetimi ve acil durum planlarına ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.
- vii. Bağımsız denetçilerin denetim izleri yönetimine ilişkin ifadelerle katılma düzeylerinin ortalamasının $\bar{X}=4,07$ olduğu görülmekte olup ölçeğin ortalamasının “katılıyorum” değer aralığında ve araştırmaya katılan

bağımsız denetçilerin denetim izleri yönetimi raporuna ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.

- viii. Bağımsız denetçilerin değişiklik yönetimine ilişkin ifadeler katılma düzeylerinin ortalamasının $\bar{X}=4,17$ olduğu görülmektedir. Bu veri doğrultusunda, ölçeğin ortalamasının “katılıyorum” değer aralığında olduğu ve araştırmaya katılan bağımsız denetçilerin denetim izleri yönetimi raporuna ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.
- ix. Bağımsız denetçilerin dış hizmet sağlayıcılarının yönetimine ilişkin ifadeler katılma düzeylerinin ortalamasının $\bar{X}=4,10$ olduğu, ölçeğin ortalamasının “katılıyorum” değer aralığına sahip olduğu ve araştırmaya katılan bağımsız denetçilerin denetim izleri yönetimi raporuna ilişkin fikirlerinin yüksek seviyede olduğu söylenebilir.
- x. Bağımsız denetçilerin hizmet yazılımlarına ilişkin ifadeler katılma düzeylerinin ortalamasının $\bar{X}=4,26$ olduğu görülmektedir. Bu değere göre ölçeğin ortalamasının “kesinlikle katılıyorum” değer aralığında olduğu ve araştırmaya katılan bağımsız denetçilerin hizmet yazılımlarına ilişkin kontrollere ait fikirlerinin yüksek seviyede olduğu söylenebilir.

Bağımsız denetçilerin e- Belge özel entegratör bilgi sistem denetimi ile ilgili ifadeler ait bilgi düzeyine ilişkin görüşlerinin cinsiyetlerine göre anlamlı bir farklılık gösterip göstermediğini görebilmek için cinsiyet gruplarına bağımsız örneklem t-testi gerçekleştirilmiş ve istatistiksel olarak anlamlı bir fark tespit edilmemiştir.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin yaş durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda yaş grupları arasında istatistiksel olarak anlamlı bir fark bulunmamıştır.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin eğitim durumlarına göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Analiz sonucunda eğitim durumlarına göre gruplar arasında istatistiksel olarak anlamlı bir fark bulunmamıştır.

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin bağımsız denetçi olarak çalışma süresine göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Çalışma süresi

için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır.

- i. Bağımsız denetçi olarak çalışma süresine göre bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin tek yönlü varyans analizi sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=4,0481$) ile 16 yıl ve üzeri ($\bar{x}=4,3804$) arasında olduğu görülmüştür ($p=0,022$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,021$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporunun*” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).
- ii. Bağımsız denetçi olarak çalışma süresine göre bağımsız denetçilerin öebd değerlendirme sınıflarından iç kontrol ve denetim mekanizmaları ile ilgili ifadelerine ilişkin tek yönlü varyans analizi sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=3,8846$) ile 16 yıl ve üzeri ($\bar{x}=4,4783$) arasında olduğu görülmüştür ($p=0,001$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,001$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD değerlendirme sınıflarından iç kontrol ve denetim mekanizmalarının*” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).
- iii. Bağımsız Denetçi olarak çalışma süresine göre bağımsız denetçilerin öebd değerlendirme sınıflarından personelin niteliği ile ilgili ifadelerine ilişkin tek

yönlü varyans analizi sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=4,0192$) ile 16 yıl ve üzeri ($\bar{x}=4,4348$) arasında olduğu görülmüştür ($p=0,042$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,026$). Bu durumda bağımsız denetçi olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD değerlendirme sınıflarından personelin niteliğinin*” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler.

- iv. Bağımsız denetçi olarak çalışma süresine göre bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerle ilişkin tek yönlü varyans analizi sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=3,8526$) ile 16 yıl ve üzeri ($\bar{x}=4,2899$) arasında olduğu görülmüştür ($p=0,026$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,048$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planlarının*” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).
- v. Bağımsız denetçi olarak çalışma süresine göre bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetimi ile ilgili ifadelerle ilişkin tek yönlü varyans analizi sonucunda anlamlı farklılığın 1-5 yıl ($\bar{x}=3,9295$) ile 16 yıl ve üzeri ($\bar{x}=4,2754$) arasında olduğu görülmüştür ($p=0,039$). Yapılan bu testin sonucunda çalışma süresi 16 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,048$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD değerlendirme sınıflarından dış hizmet*

sağlayıcılarının yönetiminin” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

- vi. Bağımsız denetçi olarak çalışma süresine göre bağımsız denetçilerin ÖEBSD değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin tek yönlü varyans analizi sonucunda anlamlı farklılığın hem 1-5 yıl ($\bar{x}=3,9327$) ile 6-10 yıl ($\bar{x}=4,2500$) arasında olduğu hemde 1-5 yıl ($\bar{x}=3,9327$) ile 16 yıl ve üzeri ($\bar{x}=4,3804$, $S=0,46386$) arasında olduğu görülmüştür ($p=0,004$). Yapılan bu testin sonucunda çalışma süresi 6-10 yıl grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,048$). Ayrıca yapılan bu testin diğer sonucunda çalışma süresi 6-10 yıl ve üzeri olan grubun ortalaması, 1-5 yıl arası olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,007$). Bu durumda bağımsız denetçi olarak çalışma süresine bağlı olarak; 16 yıl ve üzeri tecrübeye sahip olan bağımsız denetçiler 1-5 yıl tecrübeye sahip denetçilere göre ve 6-10 yıl tecrübeye sahip denetçiler 1-5 yıl tecrübeye sahip denetçilere göre “*ÖEBSD değerlendirme sınıflarından dış hizmet sağlayıcılarının yönetiminin*” bilgi sistemleri kalitesini etkilediği yönünde ki fikri daha fazla desteklemektedirler. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

Katılımcıların, araştırma kapsamında irdelenen değişkenlere ilişkin görüşlerinin denetim firmasındaki pozisyonuna göre anlamlı bir farklılık gösterip göstermediğini belirlemek amacıyla tek yönlü varyans analizi yapılmıştır. Denetim firmasındaki pozisyon için yapılan tek yönlü varyans analizinde anlamlı farklılığın hangi gruplar arasında olduğunu bulabilmek için gruplara çoklu karşılaştırma yöntemlerinden Tukey in HSD testi yapılmıştır.

- i. Denetim firmasındaki pozisyonuna göre bağımsız denetçilerin bilgi sistemleri denetiminin bağımsız denetime etkisi ile ilgili ifadelerle katılma düzeyine ilişkin yapılan tek yönlü varyans analizi sonucunda anlamlı farklılığın denetçi yardımcısı ($\bar{x}=3,9741$) ile baş denetçi ($\bar{x}=4,4044$) arasında olduğu görülmüştür ($p=0,008$). Yapılan bu testin sonucunda

denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,018$). Bu sonuç baş denetçilerin “bilgi sistemleri denetiminin bağımsız denetime etkisi” olduğu fikrine denetçi yardımcılarına göre daha fazla katıldıklarını göstermektedir. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

ii. Denetim firmasındaki pozisyonuna göre bağımsız denetçilerin ÖEBSĐ değerlendirme sınıflarından uluslararası sertifikasyonlar, sızma testi hizmeti ve BİS raporu ile ilgili ifadelerine ilişkin yapılan tek yönlü varyans analizi sonucunda anlamlı farklılığın hem denetçi yardımcısı ($\bar{x}=3,7931$) ile baş denetçi ($\bar{x}=4,6275$) arasında hemde denetçi ($\bar{x}=4,0811$) ile baş denetçi ($\bar{x}=4,6275$) arasında olduğu görülmüştür ($p=0,001$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,001$). Ayrıca denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,02$). Bu sonuca göre baş denetçilerin “*ÖEBSĐ Değerlendirme Sınıflarından Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu ile İlgili İfadelere*” denetçi yardımcılarına ve denetçilere göre daha fazla katıldıkları görülmektedir. Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$).

iii. Denetim firmasındaki pozisyonuna göre bağımsız denetçilerin ÖEBSĐ değerlendirme sınıflarından iş sürekliliği, risk yönetimi ve acil durum planları ile ilgili ifadelerine ilişkin yapılan tek yönlü varyans analizi sonucunda anlamlı farklılığın denetçi yardımcısı ($\bar{x}=3,8506$) ile baş denetçi ($\bar{x}=4,4706$) arasında olduğu görülmüştür ($p=0,029$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,029$). Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$). Bu sonuca göre baş denetçilerin “*ÖEBSĐ Değerlendirme Sınıflarından İş Sürekliliği, Risk*

Yönetimi ve Acil Durum Planları ile İlgili İfadeler” denetçi yardımcılarında daha fazla katıldıkları görülmektedir.

- iv. Denetim firmasındaki pozisyonuna göre bağımsız denetçilerin ÖEBS D değerlendirme sınıflarından denetim izleri yönetimi ile ilgili ifadelerle ilişkin yapılan tek yönlü varyans analizi sonucunda anlamlı farklılığın kıdemli denetçi ($\bar{x}=3,5500$) ile baş denetçi ($\bar{x}=4,3725$) arasında olduğu görülmüştür ($p=0,043$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, kıdemli denetçi olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,027$). Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$). Bu sonuca göre baş denetçilerin “*ÖEBS D Değerlendirme Sınıflarından Denetim İzleri Yönetimi ile İlgili İfadeler*” kıdemli denetçilere göre daha fazla katıldıkları görülmektedir.
- v. Denetim firmasındaki pozisyonuna göre bağımsız denetçilerin ÖEBS D değerlendirme sınıflarından hizmet yazılımlarına ilişkin kontroller ile ilgili ifadelerle ilişkin yapılan tek yönlü varyans analizi sonucunda anlamlı farklılığın denetçi yardımcısı ($\bar{x}=3,9310$) ile baş denetçi ($\bar{x}=4,4559$) arasında olduğu görülmüştür ($p=0,027$). Yapılan bu testin sonucunda denetim firmasındaki çalışma pozisyonu baş denetçi olan grubun ortalaması, denetçi yardımcısı olan grubun ortalamasından istatistiksel olarak anlamlı şekilde yüksek bulunmuştur ($p=0,018$). Diğer çalışma yılı grupları arasında anlamlı bir farklılık yoktur ($p>0,05$). Bu sonuca göre baş denetçilerin “*ÖEBS D Değerlendirme Sınıflarından Hizmet Yazılımlarına İlişkin Kontroller ile İlgili İfadeler*” denetçi yardımcılarında göre daha fazla katıldıkları görülmektedir.

Çalışma genel olarak değerlendirildiğinde bağımsız denetçilerin, bilgi sistemleri denetiminin bağımsız denetime etkisine dair görüşleri ele alınmış, bilgi sistemleri denetimi ile bağımsız denetim arasında anlamlı bir ilişki vardır görüşü kabul edilmiştir. Bilgi sistemleri denetiminin bağımsız denetimin bir parçası olduğuna ve bağımsız denetim sürecinde kapsamlı bir biçimde incelenmesi ve analiz edilmesi gerektiği görüşüne katılan bağımsız denetçiler; her iki denetimin uyum içerisinde yürütülmesinin daha şeffaf sonuçların ortaya çıkmasına katkı sağlayacağını kabul etmektedirler.

Bağımsız denetçiler bağımsız denetim planı oluşturulurken, denetim riskinin büyüklüğünü belirlerken bilgi sistem denetimi sonuçlarının dikkate alınması gerektiği görüşünü benimsemektedirler. Genel olarak bakıldığında bağımsız denetçilerin sorulara vermiş oldukları cevaplardan yola çıkarak bağımsız denetim ile bilgi sistem denetiminin uyumlu hale getirilmesi gerekmektedir. SPK, BDDK ve GİB 'in bilgi sistemleri denetimine dair düzenlemeleri olduğu gibi, KGK tarafından da hazırlanacak her iki denetimi uyumlu hale getiren yol gösterici nitelikte ayrıntılı bir rehber ihtiyacı vardır.

Bağımsız denetimde kanıt niteliği taşıyan e-fatura, e-defter v.b e-belgelerin elektronik ortamda iletim yöntemlerinden biride özel entegrasyondur. GİB den elde edilen bilgiye göre Türkiye'de faaliyet gösteren özel entegrasyon izni almış 92 tane kurum mevcuttur. Çalışmanın 3. bölümünde bağımsız denetçilerin e-belge özel entegratörleri bilgi sistem denetimine ilişkin bilgi düzeyleri araştırılmış %63,3'ünün e-belge özel entegratör kuruluşları hakkında bilgi sahibi oldukları ve e-belge özel entegratör bilgi sistemleri denetimi ile ilgili sorulara verilen cevaplar incelendiğinde neredeyse tamamına yakınının bilgi sistemleri denetimi hakkında fikir sahibi oldukları görülmektedir.

Araştırmaya katılan bağımsız denetçilerin %14,2'sinin bilgi sistemleri denetçi sertifikası (CISA)'na sahip oldukları, %85,8'inin ise bu sertifikaya sahip olmadıkları görülmektedir. Ülkemizde BDDK, bilgi sistemleri alanında denetim yapmak için CISA sertifikasının gerekliliğini yasal mevzuat ile zorunlu kılmıştır. Bilgi sistemleri denetçisi olabilmek için bilgi sistemleri bağımsız denetim lisans belgesi veya bilgi sistemleri denetim ve kontrol birliği (ISACA) tarafından verilen bilgi sistemleri denetçisi sertifikasına (CISA) sahip olunması gerekmektedir. Sermaye piyasası lisanslama ve sicil ve eğitim kuruluşundan elde edilen verilere göre bilgi sistemleri bağımsız denetim lisansına sahip 12 kişi bulunmaktadır. Bilgi sistemleri denetçisinin tüm dünyada olduğu gibi ülkemizde de eksikliği dikkat çekici bir durum olup, bu eksikliği gören denetçilerin CISA belgesine sahip olarak bu eksikliği gidermek için bir başlangıç yaptıkları, bu çalışmada toplam 120 bağımsız denetçinin 17'sinin CISA belgesine sahip olduğu durumu ile açıklanabilir. Bilgi sistemleri denetçiliğinde CISA belgesine sahip denetçilerin sayısının artması önemli bir açığı giderecektir. Bu çalışmada çalışma evreni olarak Ankara ilinde faaliyet gösteren bağımsız denetçiler seçilmiş olup bundan sonra yapılacak çalışmalarda evren tüm Türkiye olarak genişletilebilir.

KAYNAKÇA

- Acuner, S., (2017). *Bankacılık Hukuku*, 1. Baskı, Celepler Basın Yayın Dağıtım, Trabzon,
- Akdaş, H., (2019). *Üniversitelerin Bilgi İşlem Birimlerinin ITIL Çerçevesinde İncelenmesi ve Etkin Bir Yönetim Modeli Önerisi*. Yüksek Lisans Tezi, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, İstanbul.
- Angel, R.O., (2018). *Information Technology Control and Audit*, (50. Baskı) Taylor Francis Group, London.
- Bilgin, B. Ö., (2016). *Bilgi Teknolojileri Denetimi ve Bir Uygulama*. Yüksek Lisans Tezi, Marmara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Muhasebe Denetimi Bilim Dalı, İstanbul.
- Çölkesen, R., ve Örencik, B., (2012). *Bilgisayar Haberleşmesi ve Ağ Topolojileri*, (5. baskı), Papatya Yayınevi, İstanbul.
- Çelik, A.İ., (2016). *ASP.Net ile SQL Server Veri Tabanı Uygulamaları*, Ekin Basım Yayın Evi, Bursa,
- Database defined <<https://www.oracle.com/database/what-is-database>> (25.09.2022).
- Bourgeois D., vd., (2019). *Information Systems for Business and Beyond* , (1. baskı), Creative Commons Attribution-NonCommercial 4.0 International License.
- Bozkurt, N., (2012). *Muhasebe Denetimi*, (6. baskı), Alfa Yayınları, İstanbul , pp 29
- Böcek, B., (2014). *Bilgi Teknolojileri Denetiminin İçeriği ve Mali Denetimde Karşılıdığı Riskler*. Yüksek Lisans Tezi, Gazi Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı, Ankara.
- Çalgan, E., vd., (2008). *Muhasebe Denetimi*, (1. baskı), ISMMMO Yayın , İstanbul.
- Curtis G. ve Cobham D., (2005). *Business Information Systems: Analysis, Design and Practice*. Prentice Hall.5th Ed. [Electronic Book].
- Çelik, A., ve Akgemci, T., (2010). *Yönetim Bilişim Sistemleri*, Gazi Kitabevi, Ankara.

Difference Between Information System and Information Technology
<<https://www.geeksforgeeks.org/difference-between-information-system-and-information-technology/?ref=gcse>> (15.10.2022).

Dinç, Y., ve Cengiz, S., (2014). Muhasebe denetiminde hata ve hilenin denetçi etiği açısından incelenmesi: enron skandalı örneği. *Çankırı Karatekin Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 5(1): 230.

Drljaca, D., ve Latinović, B., (2016). Frameworks for audit of an information system in practice. *JITA Journal of Information Technology and Applications*. 6. 78-85. 10.7251/JIT1602078D.

Durmuş, A. F., ve Koca, Z., " Muhasebe İşlemlerinde Dijitalleşmenin Denetime Etkisi", 1. Uluslararası Beydağı Sosyal ve Beşeri Bilimler Kongresi Kitabı, Malatya, 2019, ss. 279-287e-Belge Özel Entegratörleri Bilgi Sistemleri Denetimi Kılavuzu, Kasım 2019.

Erdoğan, M., vd., (2018). *Denetim*, (1. baskı), Anadolu üniversitesi Yayınevi , Eskişehir.

Feyyaz Öner F., (2022). *e-Muhasebe Uygulamalarının Muhasebe Bilgi Sistemi ve Vergi Denetimi Etkileşimi Üzerine Bir Araştırma*. Yüksek Lisans Tezi, Dokuz Eylül Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı Muhasebe Programı, İzmir.

Finansal Ansiklopedi, Amerikan Yeminli Mali Müşavirler Enstitüsü (AICPA)
<<https://tr.nesrakonk.ru/american-institute-of-certified-public-accountants/>>
(15.10.2010).

Florida Tech, Information Systems vs. Information Technology
www.floridatechonline.com/blog/information-technology/information-systems-vs-information-technology/ (19.09.2022).

Gülten, S., ve Erdem, A., (2021). *Dijital Muhasebe Uygulamaları*. Gazi Kitabevi, Ankara.

Gülten, S., *e-Maliye Muhasebe Uygulamaları Eğitim Notları*, Ankara.

Güredin, E., ve Uyar, S., (2020). *Denetim ve Güvence Hizmetleri* , (15. baskı), Türkmen Yayınları, İstanbul.

Haftacı, V., (2018). *Muhasebe Denetimi*, (5. baskı), Umuttepe Yayınları, Kocaeli.

Information system<www.techwalla.com/articles/whar-are-the-six-elements-of-an-information-system> (18.10.2022).

ISACA 2010 Denetim, Güvence ve Kontrol Uzmanlarının BT Standartları, Rehberleri, Araç ve Teknikleri.

ISACA 2012 COBIT 5: A Business Framework for the Governance and Management of Enterprise IT.

ISACA 2014 CISA Review Manual.

ISACA, ITAF 3rd Ed. <[http://www.isaca.org/Knowledge-Center/Research/Documents/ITAF-3rd Edition_fm_k_Eng_0614.pdf](http://www.isaca.org/Knowledge-Center/Research/Documents/ITAF-3rd-Edition_fm_k_Eng_0614.pdf)> (12.11.2022).

ISACA Hakkında <https://www.isaca.org/why-isaca/turkish> (17.10.2022).

ISO 27001: The International Information Security Standard, <https://www.itgovernance.co.uk/iso27001> (18.08.2022).

IT Audit Manual 2017 Grant Thornton'un Eğitim Notları. Sweden.

IT Audit manual,

<https://ms.hmb.gov.tr/uploads/sites/2/2019/09/itaudit_manual_asosai.doc> (22.08.2022).

İşletmelerde “Çifte Kayıt” Gerçeği ve Hapis Cezası Riski. <<https://upaymm.com.tr/>> (15.10.2022).

Kara, R., (2019). *Bilgisayar Ağları*, (1. baskı), Nobel Yayınevi, Ankara.

Koç, S., vd., (2019). Bilişim teknolojileri (BT) denetiminde bilgi güvenliği ile ilgili uluslararası standartlar ve Türkiye'deki uyum çabalarının incelenmesi.

Uluslararası Muhasebe ve Finans Arařtırmaları Dergisi, 1(2), 121-139.KPMG, (2017). *BT Denetim Standartları ve Uygulamaları*, KPMG, İstanbul.

KPMG BT Denetim Standartları ve Uygulamaları Arařtırma Raporu 2017, <kpmg.com.tr>, (24.08.2022).

Ly-Huong T. Pham, vd., (2022). *Information Systems For Business*, (2. baskı), Libretexts, Kaliforniya.

Libretexts workforce, Identifying the Components of Information Systems <https://workforce.libretexts.org/Bookshelves/Information_Technology/Information_Systems/Information_Systems_for_Business/01%3A_What_Is_an_Information_System/01%3A_What_Is_an_Information_System/1.02%3A_Identifying_the_Components_of_Information_Systems> (10.05.2022).

Meaning and Elements of Computer System <<https://www.toppr.com/guides/accountancy/application-of-computers-in-accounting/meaning-and-elements-of-computer-system/>> (10.06.2022).

Meral E., (2016). Türkiye’de Bilgi Sistemleri Denetimi ve Kamu Gözetimi Kurumu’nun Bilgi Sistemleri Denetiminde Üstlendiđi Misyon. Uzmanlık Tezi. Ankara.

OSI Model <www.imperva.com/learn/application-security/osi-model> (15.10.2022).

Özarslan D., (2014) *Muhasebe Bilgi Sistemleri Denetimi*. Yüksek Lisans Tezi, Ankara Üniversitesi Sosyal Bilimler Enstitüsü İşletme Anabilim Dalı. Ankara.

Özbilgin, İ. G., (2009). Bilgi teknolojileri denetimi ve uluslararası standartlar. *Sayıřtay Dergisi*, Sayı 45.

Özbilgin, İ. G., (2012). Kamu kurumları açısından bilgi sistemleri denetimi, *Biliřim Dergisi*, 147, 162-166.

Özbilgin İ. G., (2016). Bilgi teknolojileri denetimi ve uluslararası standartlar. *Sayıřtay Dergisi*, 49.

Özekiciođlu, S., (2018). Yüksek denetimin tarihsel geçmiři ve avrupa birliđi’nde yüksek denetim, *Journal of Economic Policy Researches*, 5 (1), 77.

- Özer, E. (2015). Vergi incelemesinde yeni dönem: e-Defter, *Vergi Sorunları Dergisi*, 322, 65-69.
- Romney, M.B., ve Steimbart P.J., (2020), *Accounting Information Systems* , (14. baskı), Pearson Yayınları, İngiltere.
- Sayana S. A., (2002). The IS Audit Process. *Information Systems Control Journal*, 1(42),
- SAYIŞTAY 2013, *Bilişim Sistemleri Denetim Rehberi*. T.C. Sayıştay Başkanlığı,
- Sayıştay, (2013). *Bilişim Sistemleri Denetimi Rehberi*, Ankara, <http://www.sayistay.gov.tr/Tr/Upload/files/bilisim.pdf> adresinden ulaşılabilir.
- Selimoğlu, S, K., vd., (2019). *Muhasebe Denetimi*, (3. baskı), Atlas Yayınevi , Ankara.
- Selimoğlu, S.K., vd., (2019). *Bağımsız Denetim Türkiye Denetim Standartlarıyla Uyumlaştırılmış*, (3.baskı), Nobel Akademik Yayıncılık. Ankara.
- Sermaye Piyasası Kurulu, Bilgi sistemleri bağımsız denetim tebliği (III-62.2) (5/1/2018 tarihli ve 30292 sayılı Resmî Gazetede yayımlanmıştır.
- Sermaye Piyasası Kurulu, (2013). *Sermaye Piyasasında Bağımsız Denetim Standartları Hakkında Tebliğ*, Seri: X, No: 22, Ankara, 240 <http://www.spk.gov.tr/displayfile.aspx?action=displayfile&pageid=590&fn> adresinden ulaşılabilir.
- Sızma Testi Nedir? <<https://lostar.com.tr/2020/10/sizma-testi-nasil-yapilir.html>> (21.08.2022).
- Şirin, M., (2012). *Uluslararası Denetim Standartları Çerçevesinde Denetim Kanıtları, Kanıt Toplama Teknikleri ve İstatistikî Örnekleme Yöntemleri*, Hazine Bakanlığı, Ankara. <http://www.hazine.org.tr/tr/images/uluslararasi%20denetm%20standartlari.pdf> adresinden ulaşılabilir.
- Tanrıverdi, Ö., (2021). *Bağımsız Denetim Sürecine Kanıt toplama ve Görüş Oluşturmada Analitik İnceleme Tekniklerinin Uygulanması*. Doktora tezi), Başkent Üniversitesi Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı , Ankara.

Toroslu, M.V., (2016). *Finansal Tablolar Denetimi Kavramlar-Denetim Süreci-Denetim Teknikleri*, (2.Baskı), Seçkin Yayıncılık, İstanbul.

Türk Standardları Enstitüsü, 2013, Sızma Testi Teknik Kriterleri Programı, <https://statik.tse.org.tr/upload/tr/dosya/icerikyonetimi/2224/01042015105039-3.pdf>, (18.08.2022).

Uyanık, A., (2001). *Denetim, Muhasebe ve Vergilendirme*, (1.baskı), Beta Basım A.Ş, İstanbul.

Vergi Usul Kanunu Genel Tebliği (Sıra No: 509)

Yalkın, L. D., (2011). *Bilgi Teknolojileri Denetimi. Kavramsal Çerçeve, Aşamaları, Sınırları, Sorunları*. ANKARA.

Yıldırım, S., (2017). *Sermaye Piyasası Kuruludenetleme Dairesi, Bilgi Sistemleri Denetim Süreçleri Yeterlik Etüdü*. İstanbul.

EKLER

EK 1. e-Belge Özel Entegratörleri Bilgi Sistemleri Denetimi Kılavuzu

ÖEBSD Değerlendirme Sınıfları

Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu (ÖEBSD_SER)

Bu değerlendirme sınıfı, özel entegratörlerin sağlaması gereken uluslararası sertifikasyonların varlığı ve uygunluğu ile sızma testlerinin uygunluğunun kontrol edilmesini amaçlamaktadır. Bu sınıf altında iki alt bileşen tanımlanmıştır:

ÖEBSD_SER.1 Bu değerlendirme alt bileşeninde denetçiden özel entegartörün aşağıda uluslararası sertifikasyonları sahip olduğunu teyit etmesi istenmektedir:

ISO/IEC 20000 Bilgi Teknolojileri Hizmet Yönetim Sistemi Belgesi

ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Belgesi

ISO 22301 İş Sürekliliği Yönetim Sistemi Belgesi

Son yapılan sızma testi raporu

Güncel BİS Raporu

ÖEBSD_SER.2 Bu değerlendirme alt bileşeninde denetçiden, özel entegratörün iç kontrol ve denetim süreçlerinin varlığını ve çıktılarının uygunluğunu kontrol etmesi beklenmektedir.

Değerlendirme alt bileşenlerine ilişkin kontrol tabloları eklerde verilmiştir.

Personelin Niteliği (ÖEBSD_PER)

Bu değerlendirme sınıfında, özel entegratörün, verdiği özel entegratörlük hizmetine uygun nitelikte ve sayıda personel istihdam edip etmediği kontrol edilecektir.

Sistem ve Güvenlik Değerlendirme Sınıfı (ÖEBSD_SIS)

Bu değerlendirme sınıfı, özel entegratörlerin bilgi sistemlerinde uyması gereken alt yapının, sistem mimarisi ve benzeri her türlü fiziki unsur ile iş sürekliliğinin temininin,

gerekli güvenlik ve risk değerlendirme süreçlerinin oluşturulmasının, işletilmesinin, değişiklik yönetiminin, denetim izlerinin oluşturulmasının ve dışarıdan hizmet alınması durumundaki gerekliliklerin kontrol edilmesini amaçlamaktadır.

Bu değerlendirme sınıfının oluştuğu 7 alt bileşen aşağıda açıklanmıştır:

ÖEBSD_SIS.1 Fiziki Şartlar ve Güvenlik Tedbirleri: Özel entegratörün sağlaması gereken uluslararası sertifikasyonları varlığı ve uygunluğu ile sızma testlerinin uygunluğu kontrol edilecektir.

ÖEBSD_SIS.2 Erişim Güvenliği: Özel entegratörün bilgi sistemlerinin sağlaması gereken fiziki ve elektronik erişim güvenliği kontrol edilecektir.

ÖEBSD_SIS.3 İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları: Özel entegratörün “İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları” kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.4 Değişiklik Yönetimi: Özel entegratörün “Değişiklik Yönetimi” kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.5 Denetim İzleri Yönetimi: Özel entegratörün “Denetim İzleri Yönetimi” kurallarına uygunluğu kontrol edilecektir.

ÖEBSD_SIS.6 Dış Hizmet Sağlayıcılarının Yönetimi: Özel entegratörün “Dış Hizmet Sağlayıcılarının Yönetiminin” kurallara uygunluğu kontrol edilecektir.

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller: Özel entegratörün hizmetlerinde kullandığı uygulama yazılımlarının, ilgili GİB kılavuzları, e-Fatura, e-Saklama, e-Arşiv, e-İrsaliye, e- Defter ve e-imza standartları ve hizmetin akışına uygun normları taşıyıp taşımadığı kontrol edilecektir.

Değerlendirme alt bileşenlerine ilişkin kontrol tabloları eklerde verilmiştir.

EK 1. ÖEBSD Değerlendirme Sınıfları Kontrol Tabloları

ÖEBSD_SER.1: Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS Raporu

Özel entegratörün sağlaması gereken uluslararası sertifikasyonların varlığı ve uygunluğu ile sızma testlerinin uygunluğu aşağıdaki tabloya göre kontrol edilecektir. Sertifika belgeleri Değerlendirme Raporu ekinde yer almalıdır. Dış hizmet alımı

durumunda, ilgili kontrol ve testler, dış hizmet alımının yapıldığı lokasyonlarda da, özel entegratörlük faaliyeti ile sınırlı olmak üzere, tekrarlanacaktır.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SER.1: Uluslararası Sertifikasyonlar, Sızma Testi Hizmeti ve BİS		
Kontrol No	Kontrol Maddesi	Sonuç
A1	ISO / IEC 20000 Sertifikası mevcut ve denetim tarihinde geçerli mi?	
A2	ISO 22301 Sertifikası mevcut ve denetim tarihinde geçerli mi?	
A3	ISO / IEC 27001 Sertifikası mevcut ve denetim tarihinde geçerli mi?	
A4	ISO / IEC 27001 Sertifikası, bilgi sistemlerini ve bu kılavuzda belirtilen kritik varlıkları işleyen ve kullanan süreçleri kapsıyor mu?	
A5	Son yapılan sızma testi tarihinden itibaren geçen süre 1 yıldan kısa mıdır?	
A6	Sızma testinde veri tabanı sistemleri incelenmiş midir?	
A7	Sızma testinde ağ ve iletişim altyapısı güncel saldırı yöntemlerine göre test edilmiş midir?	
A8	Sızma testinde işletim sistemleri ve platformlar güvenlik açıkları açısından değerlendirilmiş midir?	
A9	Sızma testinde uygulamalar güncel saldırı yöntemlerine göre incelenmiş midir?	
A10	Sızma testi bulguları arasında bilgi sistemlerini güvenliğini tehdit eden kritik düzeyde bir açık olmadığını teyit ettiniz mi?	

Özel entegratörün iç kontrol ve denetimi bu tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SER.2: İç Kontrol ve Denetim Mekanizmaları		
Kontrol No	Kontrol Maddesi	Sonuç
B1	İç kontrol ve iç denetim dokümanı oluşturulmuş ve uygulanıyor mu?	
B2	İç ve dış denetimde kullanılmak üzere iç kontrol sonuçlarının nasıl raporlanacağı belirlenmiş mi?	
B3	İç kontrol dokümanları ile iş sürekliliği dokümanları birbiriyle uyumlu mu?	
B4	İç kontrol denetimleri periyodik biçimde yapılmış ve denetim sonuçları raporlanmış mı?	
B5	İç kontrol denetim sonuçlarının gereği yapılmış mı?	

ÖEBSD_PER: Personelin Niteliği

Özel entegratörün iç kontrol ve denetimi bu tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_PER: Personelin Niteliği		
Kontrol No	Kontrol Maddesi	Sonuç
C1	Bilgi sistemlerinde çalıştırılan personel sayısı yeterli midir?	
C2	Ağ ve ağ güvenliği uzmanı, veri tabanı uzmanı, kalite sistemleri uzmanı, yazılım geliştirme uzmanı, konfigürasyon yöneticisi ve test uzmanı rollerinin her birisi için ayrı bir kişi olmak üzere en az 1 personel bulunuyor mu?	
C3	Bilgi sistemleri organizasyon şeması ve bağlı kadro planı yönetim kurulu kararıyla belirlenmiş mi?	
C4	Son denetim tarihinden bugüne kadar istihdam edilen yeni personel ile işten ayrılan personelin GİB'e zamanında bildirilmiş olduğu teyit edilebiliyor mu?	

ÖEBSD_SIS.1: Fiziki Şartlar ve Güvenlik Tedbirleri

Özel entegratörün bilgi sistemlerinin sağlaması gereken fiziki ve güvenlik şartları aşağıdaki tabloya göre kontrol edilecektir. HSM'lere ilişkin sertifika belgeleri Değerlendirme Raporu ekinde yer almalıdır. Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.1: Fiziki Şartlar ve Güvenlik Tedbirleri		
Kontrol No	Kontrol Maddesi	Sonuç
D1	Özel entegratör münhasıran faaliyetine ayrılmış bir veri tabanı çalıştırıyor mu?	

D2	Veri tabanının çalıştığı sunucu kümesinin uygulama dışında erişime açık bırakılmadığı teyit edilebiliyor mu?	
D3	Veri tabanının çalıştığı sunucu kümesinin veri tabanı portları dışında erişime açık olmadığı teyit edilebiliyor mu?	
D4	Veri tabanı üzerinde “linked server” yapılanmasının olmadığı kontrol edildi mi?	
D5	Veri tabanının çalıştığı sunucu kümesi üzerinde başka servisler veya uygulamaların çalıştırılmadığı kontrol edildi mi?	
D6	Kriptografik anahtarlar, FIPS 140-2 Düzey 3 veya EAL 4+ sertifika sahibi sadece özel donanım güvenlik modüllerinde (HSM) mi barındırılıyor?	
D7	Hassas veriler (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanıyor mu?	
D8	Hassas verilere herhangi bir personelin tek başına erişim yetkisi yoktur.	
D9	Sistemlerde bulunan ve veri gizliliği amacıyla şifreli tutulan verilen veriler için kullanılan şifreleme yöntemleri AES 256, RSA2048 ve hash algoritmasında SHA-2 olacak biçimde uygulanmış mıdır?	
D10	Denetim izi için tutulan kayıtlar, geçmişteki bir olayın izlenmesi için yeterli düzeyde veri içermekte midir?	
D11	Denetim izi için tutulan kayıtlar, ayrı bir sunucu kümesinde, veri bütünlüğü dikkate alınarak saklanıyor mu?	
D12	Denetim izi için tutulan kayıtlar için, olağan dışı hareketleri anında tespit edip otomatik uyarı üreten mekanizmalar kurulmuş mu?	
D13	Özel entegratör ile GİB arasında iletişim amacıyla kullanılan erişim hatları için kapasitesi ve hattın yedeklenmesi bakımından yeterli düzeyde mi?	
D14	Bilgi sistemleri ağ ve uygulama topolojileri ile varlıklara erişim için yetkilendirilmiş tüm kullanıcıların isimleri güncel ve güvenli biçimde tutuluyor mu?	
D15	Veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin durmasına izin verecek bir yapılanma olmadığı kontrol edildi mi?	

D16	Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gereklilikleri sağlanmış mıdır?	
D17	Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalarda, 7x24 görüntü kaydı yapılıyor mu?	
D18	Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalardaki görüntü kayıtları en az 6 ay süreyle saklanıyor mu?	
D19	Bilgi sistemlerinde kullanılan aktif ağ cihazları, güvenlik duvarları ve sunucu veya kişisel bilgisayarlarda kullanılan her türlü 3. parti yazılımın son güncel sürümleri kullanılıyor mu?	
D20	Bilgi sistemlerinde kullanılan aktif ağ cihazlarının, güvenlik duvarlarının, sunucu, kişisel bilgisayarların arızası veya bakımı nedeniyle 3. kişilerin erişimine açılması halinde, işlem süresince yeterli gözetimin yapılıp olay kayıtları tutuluyor mu?	

ÖEBSD_SIS.2: Erişim Güvenliği

Özel entegratörün bilgi sistemlerinin sağlaması gereken fiziki ve elektronik erişim güvenliği aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.2: Erişim Güvenliği		
Kontrol No	Kontrol Maddesi	Sonuç
E1	Sistem odaları ve kritik odalara erişim yetkilendirmeleri ile personel kadro planındaki roller uyumlu mu?	

E2	Sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtlar güvenli biçimde tutuluyor mu?	
E3	Sistem odaları ve kritik odalara erişim için iki faktörlü kimlik doğrulama mekanizması kullanılmış mı?	
E4	Sistem odaları ve kritik odalara erişimde en az iki yetkili ilkesi uygulanıyor mu?	
E5	Sistem odaları ve kritik odaların kapıları endüstri standartlarına uygun çelik kapılarla yapılıyor mu?	
E6	Sistem odaları ve kritik odalara her zaman en az iki yetkilendirilmiş kişinin bir arada olmasıyla erişimin mümkün olacağı mekanizma kurulmuş mu?	
E7	Fiziki erişim için kapı geçiş sistemlerinde yapılan yetkilendirme için ayrılaştırılmış roller ve en az iki yetkili ilkesi uygulanıyor mu?	
E8	Veri tabanlarına, uygulamalara ve her türlü aktif cihaza (sunucular, aktif ağ cihazları, güvenlik duvarları vb.) erişimde kullanılan yönetici şifreleri ile kullanıcı şifreleri ayrılaştırılmış mı?	
E9	Tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş mu?	
E10	İşten ayrılan veya kötü niyetli bir yetkilinin tek başına, sistemlere erişimi ortadan kaldıracak veya yeniden çalıştırılmayacak biçimde bir sistemi durdurmasının engellenmesi için tedbirler alınmış mı?	
E11	Yönetici ve uygulama şifreleri, endüstriyel güvenli şifre standartlarını sağlayacak biçimde belirleniyor mu?	
E12	Yönetici ve uygulama şifreleri, endüstriyel güvenli şifre standartlarını sağlayacak biçimde belirlenen sürelerde yenileniyor mu?	
E13	Veri Aktarım Protokolü ve mükellef ile arasında çalışan haberleşme protokolüne dair tutulan güvenlik parametreleri, bu parametrelere erişim yetkileri ve bunların (parametrelerin görüntülenmesi, güncellenme sıklığı vb.) korunması sağlanıyor mu? Yönetici şifrelerinin yedekleri güvenli biçimde tutuluyor mu?	

ÖEBSD_SIS.3: İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları

Özel entegratörün “İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları” kurallarına uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.3: İş Sürekliliği, Risk Yönetimi ve Acil Durum Planları		
Kontrol No	Kontrol Maddesi	Sonuç
F1	İş sürekliliği prosedürü oluşturulmuş mu?	
F2	İş sürekliliği kapsam ve içerik yönünden amacına hizmet eder nitelikte mi?	
F3	Üst yönetim, iş sürekliliği prosedürünün çalıştırılmasından birinci derecede sorumlu tutulmuş ve bu sorumluluğunu yerine getirmiş mi?	
F4	Özel entegratör, bir risk yönetim planı oluşturmuş mu?	
F5	Risk yönetimi kapsam ve içerik yönünden amacına hizmet eder nitelikte mi?	
F6	Risk değerlendirme tablosunda olasılık ve etki değerlendirilmesi yapılmış mı?	
F7	Niceliksel olarak risklerin beklenen parasal değeri hesaplanmış mı?	
F8	Son denetim tarihinden bugüne kadar ki kayıtlara göre, hizmetin sürekliliği gerçekleşmesiyle güncel BİS raporu ve bu Kılavuzda verilen süreler uyumlu mudur?	
F9	Hizmetin sürekliliğinin gerçekleşmesine ilişkin kayıtlar Uptime Institute Tier 2 standartlarına uygun tutuluyor mu?	
F10	Varlık envanteri, varlıklara yönelik tehditler, tehditlerin risk seviyeleri ve uygulanacak eylemler risk yönetim planında yer alıyor mu?	

F11	Bilgi sistemleri ve tüm operasyonel süreçlere ilişkin riskleri tespit ve analiz edilerek, ölçme, izleme, kontrol etme ve raporlama işlemleri yerine getiriliyor mu?	
F12	Donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olaylar risk yönetim planına dâhil edilmiş mi?	
F13	Özel entegratör 3. taraflara doğabilecek zararları karşılamak amacıyla mesleki sorumluluk sigortası yaptırmış mı?	
F14	Bilgi sistemlerine ilişkin hizmeti etkileyen olayların vuku bulması durumunda veya sistemlerde kayda değer bir değişiklik öncesinde veya yeni tehditlerin ortaya çıkması halinde, alınacak eylemler açıkça planlanmış mıdır?	
F15	Risk yönetim planı yılda en az bir kez olmak üzere üst yönetim tarafından gözden geçirilerek güncellenmeye yönelik çalışma yapıyor mu?	
F16	Yılda 1 kez olmak üzere, bilgi sistemleri iş sürekliliği testleri ve acil durum planı tatbikatı gerçekleştirilerek kayıt altına alınmakta mı?	
F17	Veri tabanının etkin ve verimli çalışmasını temin etmek üzere, düzenli aralıklarla bakım, iyileştirici indeksleme yapılıyor mu?	
F18	Bilgi sistemlerinin çıktı performansı hedefi düzenli aralıklarla gözden geçirilip ihtiyaç halinde iyileştirici faaliyetler için kararlar alınıyor mu?	
F19	Bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet vermez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanmış mı?	
F20	Acil durum planında, olaylar, sistemler üzerindeki etkileri, aşamaya bağlı gelişimleri veya kök nedenlerine göre sınıflandırılmış mı?	
F21	Acil durum planında, olaya karşı alınacak tedbirler ve yapılacaklar, olay veya sınıf bazında ele alınmış mı?	
F22	Acil durum planında, olaya müdahale, kök nedeninin bulunarak ortadan kaldırılması, belirlenen sürenin aşılması halinde FKM'ye geçiş gibi acil durumun yönetim adımları, alt süreçler, süreç sorumluları, karar verici yetkililer, ulaşılamayan hallerde yedek aktörler tanımlanmış mı?	

F23	Acil durum planı, belirlenen süre içinde hizmetin özel entegratörün merkezinden veya felaket kurtarma merkezinden (FKM) yeniden verilmeye başlanmasına ilişkin eylem adımlarını yeterli ayrıntıda içeriyor mu?	
F24	Acil durum planında, hizmetin yeniden devreye alınmasından sonra, veri kaybı veya maddi kayıp olup olmadığı, olayın kök nedeni, iş sürekliliği, risk yönetimi, acil durum planları veya fiziki altyapıda önceden saptanamamış iyileştirilmesi gerekli görülen hususların tespitine yönelik ayrıntılı bir olay sonrası değerlendirme yapılması planlanmış mı?	
F25	Olay sonrası değerlendirme tutanakları ile olaya ilişkin sistemlerdeki her türlü denetim izi, denetçilere veya ihtiyaç halinde adli makamlara sunulmak üzere güvenli biçimde saklanıyor mu?	
F26	Olay halinde, GİB veya adli makamların bilgilendirilmesi konusuna acil durum planında yer verilmiş mi?	
F27	FKM, güncel BİS raporuyla uyumlu yeterli fiziki altyapıya ve özelliklere sahip mi?	
F28	FKM, güvenlik ve hizmetin çeşitliliği ve niteliği bakımlarından, merkez bilgi sistemleriyle aynı düzeyde mi?	
F29	FKM uygun bir yerde konumlandırılmış mı?	
F30	Veri yedekleri güncel BİS raporu ve bu Kılavuzla uyumlu biçimde FKM'ye alınıyor mu?	

ÖEBSD_SIS.4: Değişiklik Yönetimi

Özel entegratörün “Değişiklik Yönetimi” kurallarına uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır.

Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.4: Değişiklik Yönetimi		
Kontrol No	Kontrol Maddesi	Sonuç
G1	Değişiklik yönetimi için bir prosedür oluşturulmuş mu?	
G2	Kullanıcı değişiklik kabul onayı var mı?	
G3	Değişiklik yönetimi prosedürü kapsam ve içerik yönünden amacına hizmet eder nitelikte mi?	
G4	Değişiklik yönetimi prosedüründe, bilgi sistemlerinde yer alan tüm donanım ve yazılımın her türlü bakım, yama ve değişikliği kapsamında yer alıyor mu?	
G5	Özel entegratör, yazılım geliştirme faaliyetinde, derlenmiş yazılım ve yazılımın tüm alt bileşenleri ile kaynak kodları geçmiş sürümleriyle birlikte yönetiyor mu?	
G6	Derlenerek bütüne dâhil edilen yazılım bileşenlerinin, ne zaman ve kim tarafından derlendiği ve bütüne dâhil edildiğinin tarihçesi tutuluyor mu?	
G7	Yazılım geliştirme ve sürüm yönetimi platformunda, geliştiriciler rollerine göre ayrıştırılmış yetkilerle tanımlanmış mı?	
G8	Derlenen yeni bir yazılım sürümü için, hangi testleri geçmesi gerektiği ve testin kimler tarafından yapılacağı önceden belirlenerek kayıt altına alınmış mı?	
G9	Test ortamı ile canlı ortam ağ erişimi düzeyinde birbirlerinden ayrılmış mı?	
G10	Test ortamında kullanılan veriler, gizlilik ve kişisel mahremiyete hâle getirmeyecek nitelikte midir?	
G11	Testleri başarıyla geçtiği halde canlı ortamda doğru çalışmayan bir sürümden geri dönüşe ilişkin plan yapılmış mı?	
G12	Geri dönüş planında, doğru çalışmayan sürümün canlı ortamda bulunduğu süre içinde veri kaybı, hatalı veya eksik işlem gibi sorunlar yaratıp yaratmadığının tespit edilerek kayıt altına alınması dikkate alınmış mı?	

ÖEBSD_SIS.5: Denetim İzleri Yönetimi

Özel entegratörün “Denetim İzleri Yönetimi” kurallarına uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.5: Denetim İzleri Yönetimi		
Kontrol No	Kontrol Maddesi	Sonuç
H1	Denetim İzleri Yönetimi için bir prosedür oluşturulmuş mu?	
H2	Denetim İzleri Yönetimi prosedüründe, denetim izlerinin oluşturulması ve güvenli saklanmasına ilişkin yeterli ayrıntıya yer verilmiş mi?	
H3	Denetim İzleri Yönetimi prosedüründe, denetim izlerine bağlı şüpheli olarak nitelendirilecek olaylar yeterli ayrıntıda tanımlanmış mı?	
H4	Denetim izlerinde, işlemi gerçekleştiren uygulama, işlemi gerçekleştiren ve varsa onaylayan yetkili kişiler veya yetkisiz erişim kayıtları, işlemin açıklaması, yapılan işlemin zaman bilgisi, işlemin olumlu veya olumsuz sonucu, etkilenen veri ve sistemlerin bilgisi yer alıyor mu?	
H5	Denetim izlerinde hassas bir veri kaydının geçmediği teyit edildi mi?	
H6	Veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl olduğu ve saklandığı kayıtlar altına alınmış mı?	
H7	Denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınmış mı?	

H8	Denetim izlerinin en az 10 yıl süreyle güvenli biçimde saklanması için yeterli altyapı oluşturulmuş mu?	
H9	Özel entegratör, GİB ile arasında çalışan Veri Aktarım Protokolü ve mükellef ile arasında çalışan güvenli haberleşme protokolüne dair tüm işlem kayıtlarını, bütünlüğünü de koruyacak biçimde 10 yıl süreyle saklıyor mu?	
H10	Denetim izlerini aktif olarak analiz eden ve şüpheli olay halinde SMS, e-posta gibi otomatik uyarı veren mekanizmalar var mı?	
H11	Ayrıcalıklı yetkiye sahip olanlarca dahi denetim izlerinin değiştirilememesi veya değiştirilmesi halinde tespiti amacıyla 5651 Sayılı İnternet Ortamında Yapılan Yayınların Düzenlenmesi ve Bu Yayınlar Yoluyla İşlenen Suçlarla Mücadele Edilmesi Hakkında Kanun uyarınca gerekli tedbirler alınmış mı?	

İ. ÖEBSD_SIS.6: Dış Hizmet Sağlayıcılarının Yönetimi

Özel entegratörün “Dış Hizmet Sağlayıcılarının Yönetiminin” kurallara uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.6: Dış Hizmet Sağlayıcılarının Yönetimi		
Kontrol No	Kontrol Maddesi	Sonuç
I1	Özel entegratör dış hizmet alımı yapıyorsa bir sözleşmesi var mı?	
I2	Bu sözleşmede alınan hizmetin türü, konusu, kapsamı, işin süresi, tarafların açık unvan ve adresleri, hak ve sorumlulukları yer alıyor mu?	

I3	Mevcut ve yürürlükte olmayan tüm sözleşmeler 10 yıl süreyle saklanıyor mu?	
I4	Alınan hizmetin niteliğine bağlı olarak, nedeniyle, ÖEBSD_SER.1, SER. 2, SIS.5, ÖEBSD_SIS.1, ÖEBSD_SIS.2, ÖEBSD_SIS.3, ÖEBSD_SIS.4 kontrollerinin bir bölümü veya tamamı için dış hizmet sağlayıcısının yerinde denetimi yapıldı mı?	
I5	Bir dış hizmet sağlayıcısında yerinde yapılan denetim kayıtlarına alınarak denetim raporuna eklendi mi?	
I6	Dış hizmet sağlayıcısının merkezi yurt içinde mi?	
I7	Dış hizmet sağlayıcısının FKM'si bu kılavuz hükümlerine uygun nitelikte mi?	
I8	Dış hizmet sağlayıcısının, özel entegratör için verdiği hizmetler için ayrıca bir taşeron kullanmadığı teyit edildi mi?	
I9	Özel entegratör, dış hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla yerinde denetliyor mu?	
I10	Özel entegratör, dış hizmet sağlayıcısını tedarikçi performansı açısından düzenli aralıklarla değerlendiriyor mu?	
I11	Dış hizmet sağlayıcısı denetim ve değerlendirmeleri kayıt altına alınmış mı?	
I12	Dış hizmet sağlayıcısı denetim ve değerlendirmeleri sonucu karara bağlanan iyileştirme önerileri izlenmiş mi?	

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller

Özel entegratörün “Hizmet Yazılımlarına İlişkin Kontroller” kurallara uygunluğu aşağıdaki tabloya göre kontrol edilecektir.

Denetçi, tablonun Sonuç Sütununa, satırda yer alan soruya olumlu cevap verebiliyorsa (E), olumsuz cevap veriyorsa (H), kanaat oluşturamamışsa (K), kanaat oluşturmasına imkân verecek verilere ulaşamadıysa (G) harfini yazacaktır.

Denetçi, (E) olarak cevap vermediği kontrol maddelerinin her biri için, cevap gerekçesini anlaşılır biçimde bu tablonun altında maddeler halinde açıklayacaktır. Denetimi dış hizmet alınan bir sağlayıcıda kontrol maddeleri için, denetimin yapıldığı dış hizmet sağlayıcısının unvanı açıklama olarak yazılmalıdır.

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller		
e-Fatura		
Kontrol No	Kontrol Maddesi	Sonuç
	1.Güvenlik	
J1	Her kullanıcı sadece kendi firması adına fatura gönderebilmekte mi?	
J2	Her kullanıcı sadece kendi firmasının alıcısı veya satıcısı olduğu faturaları görebilmekte mi?	
J3	Her kullanıcı sadece kendi firması adına uygulama yanıtı gönderebilmekte mi?	
J4	Her kullanıcı sadece kendi firmasının alıcısı veya satıcısı olduğu faturalara verilen uygulama yanıtlarını görebilmekte mi?	
	2.İşlem Kayıtlarının Saklanması	
J5	Kullanıcıların yaptığı tüm işlemlerin kayıtları saklanmakta mı?	
J6	Kullanıcıların yaptığı tüm işlemleri içeren kayıtların değişmezliği sağlanmakta mı?	
J7	Sistemlerin yazılım ve donanım alt yapısının Türkiye Cumhuriyeti sınırları içerisinde ve Türkiye Cumhuriyeti Kanunlarının geçerli olduğu yerlerde mi bulunuyor?	
J8	Saklama hizmeti kapsamında GİB ile entegrasyon sağlandı mı?	
	3. Standartlara Uyum	
J9	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL faturalar son halinde saklanmadan ve gönderilmeden önce GİB tarafından yayınlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
J10	Özel entegratör tarafından imzalanmayıp farklı kanallardan imzalı olarak alınan faturalar son halinde saklanmadan ve gönderilmeden önce imza kontrolünden geçirilmekte mi?	

J11	Özel entegratör tarafından imzalanan faturalar imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
J12	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleri kontrol edilmekte mi?	
J13	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleriyle CRL ve OCSP sonuçları kontrol edilmekte mi?	
J14	Fatura ve uygulama yanıtlarının gönderimi için oluşturulan zarflar GİB'e gönderilemezse müşterilerin müdahalesine gerek kalmadan bir süre sonra yeniden denenmekte mi?	
J15	Gönderilen fatura veya uygulama yanıtlarının zarf durum sorguları gönderim anından itibaren hemen ve sık sık yapılmamakta, sadece gönderim tarihinden itibaren 24 saat içinde GİB'den ve alıcıdan sistem yanıtı gelmeyen zarfların durumları GİB'den kontrol edilmekte ve en sık 5 saatte bir sorgulanmakta mı?	
J16	GİB tarafından iletilen zarflar hemen kontrol edilip işlenmemekte, kaydedilip hemen dönülmekte, kontrol ve işleme daha sonra yapılmakta mı?	
J17	GİB tarafından iletilen zarflar kontrol edilip işlendikten sonra hatalı veya hatasız olarak sistem yanıtı dönülmekte mi?	
J18	Oluşturulan sistem yanıtlarının gönderilip gönderilemedikleri veya gönderildikten sonra başarıyla işlenip işlenemedikleri belirli aralıklarla sorgulanarak yeniden gönderilmekte mi?	
J19	Alınan zarflar kontrol edilirken GİB tarafından yayınlanan güncel şema kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
J20	Alınan zarflar kontrol edilirken GİB tarafından yayınlanan güncel şematron (schematron) kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
J21	Alınan zarflar kontrol edilirken fatura ve uygulama yanıtları için imza olup olmadığı, varsa geçerli olup olmadığı kontrol edilmekte ve geçerli imzalar için geçerli, geçersiz imzalar için geçersiz şekilde sistem yanıtı dönülmekte mi?	

J22	Alınan fatura veya uygulama yanıtları için oluşturulan sistem yanıtları sadece sistem tarafından otomatik olarak oluşturabilmekte, kullanıcıların web servis gibi yöntemlerle sistem yanıtı zarfları göndermesine izin verilmemekte mi?	
J23	Gelen temel faturalara uygulama yanıtı oluşturulmasına izin verilmemekte mi?	
J24	Gelen ticari faturalara zarfın alınma zamanından itibaren 8 gün içinde uygulama yanıtı oluşturulabilmekte daha sonra uygulama yanıtı oluşturulamamakta mı?	
J25	Gelen ticari faturalara zarfın alınma zamanından itibaren 8 gün içinde uygulama yanıtı gönderilebilmekte daha sonra uygulama yanıtı gönderilmekte mi?	
J26	Gelen faturalara uygulama yanıtı oluşturulup oluşturulamayacağı kontrol edilirken faturanın alındığı saat kontrol edilmemekte uygulama yanıtının 8. günde 23:59'a kadar oluşturulmasına izin verilmekte mi?	
J27	Gelen ticari faturalara bir defa uygulama yanıtı verildiğinde bir daha uygulama yanıtı oluşturulmasına izin verilmemekte mi?	
J28	Gelen faturaların içindeki XSLT fatura şablonlarındaki hatalar nedeniyle görüntülenemeyen faturalar için GİB'in e-Fatura paketlerinde önerdiği gibi bir varsayılan XSLT fatura şablonu kullanılabilmekte, en azından fatura numarası, fatura tutarı, fatura tarihi, notlar gibi temel bilgilerin görüntülenmesi sağlanabilmekte mi?	
J29	Gönderilen ticari faturalara gelen uygulama yanıtları alıcının gönderilen zarfa gönderdiği sistem yanıtının özel entegratör tarafından alınma zamanından 8 gün sonrasına kadar kabul edilmekte, daha sonra gelen uygulama yanıtları kabul edilmemekte mi?	
J30	Gönderilen ticari faturaya daha önce uygulama yanıtı geldiyse gelen uygulama yanıtı kabul edilmemekte mi?	

J31	Gönderilen faturalara ve uygulama yanıtlarına GİB veya alıcı tarafından hatalı sistem yanıtı dönülmesi durumunda yeni fatura ve uygulama yanıtı oluşturulması gerekmeyen durumlarda yeni fatura ve uygulama yanıtı oluşturulması zorlanmadan mevcut fatura ve uygulama yanıtı farklı bir zarfa konarak gönderilebilmekte mi?	
J32	Gönderilen fatura ve uygulama yanıtlarının gönderim sonucu belirlenene kadar veya başarılı olduktan sonra yeniden başka bir zarfla gönderilmesine izin verilmemekte mi?	
J33	Özel entegratör, müşteri firmanın istemesi durumunda faturalarını kendi mali mührüyle imzalamasına imkân sağlamakta mı?	
	4. Hizmetin Kapatılması	
	Hizmeti kapatmak isteyen müşteri için GİB'e kapatma isteği gönderilmekte mi?	
J35	Hizmeti kapatmak isteyen müşterilere fatura ve uygulama yanıtları UBL ya da zarf olarak XML formatında teslim edilmekte mi?	

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller		
e-Arşiv		
Kontrol No	Kontrol Maddesi	Sonuç
	1. Güvenlik	
K1	Her kullanıcı sadece yetkisi olduğu firma adına fatura gönderebilmekte mi?	
K2	Her kullanıcı sadece kendi firması tarafından oluşturulan faturaları görebilmekte mi?	
K3	Her kullanıcı sadece kendi firması adına e-Arşiv raporu oluşturabilmekte mi?	
K4	Her kullanıcı sadece kendi firmasına ait e-Arşiv raporlarını görebilmekte mi?	
	2. İşlem Kayıtlarının Saklanması	
K5	Kullanıcıların yaptığı tüm işlemlerin kayıtları saklanmakta mı?	

K6	Kullanıcıların yaptığı tüm işlemleri içeren kayıtların değişmezliği sağlanmakta mı?	
	3. Standartlara Uyum	
K7	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL faturalar son halinde saklanmadan önce GİB tarafından yayınlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
K8	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL faturalar son halinde saklanmadan önce GİB tarafından yayınlanan güncel şema ve şematron (schematron) kontrollerine ilave olarak, e-Arşiv Raporunun gereksinimlerine göre ek kontrollerden geçirilmekte mi?	
K9	Özel izinle PDF formatında fatura gönderen mükelleflerin PDF faturaları fatura bilgilerini içeren bir UBL PDF'e eklenmiş olarak GİB'in yayınladığı standartlara uygun olarak (PADES yöntemi ile) imzalanmakta mı?	
K10	e-Arşiv Raporu oluşturulduktan sonra GİB'e gönderilmeden önce GİB tarafından yayınlanan güncel şema kontrolünden geçirilmekte mi?	
K11	e-Arşiv Raporu oluşturulduktan sonra GİB'e gönderilmeden önce GİB tarafından yayınlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
K12	Özel entegratör tarafından imzalanmayıp farklı kanallardan imzalı olarak alınan faturalar son halinde saklanmadan ve gönderilmeden önce imza kontrolünden geçirilmekte mi?	
K13	Özel entegratör tarafından imzalanan faturalar imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
K14	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleri kontrol edilmekte mi?	
K15	Özel entegratör tarafından imzalanan faturalar imzalanırken imza sertifikasının geçerlilik süreleriyle CRL ve OCSP sonuçları kontrol edilmekte mi?	

K16	e-Arşiv Raporları imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
K17	Sistemde birden çok faturanın aynı ETTN ile kaydedilmesine izin verilmemekte mi?	
K18	Sistemde aynı mükellefe ait aynı fatura numarası ile birden fazla fatura kaydedilmesine izin verilmemekte mi?	
K19	Özel entegratör, müşteri firmanın istemesi durumunda faturalarını kendi mali mührüyle imzalamasına imkân sağlamakta mı?	
K20	e-Arşiv Fatura özel entegratör üzerinden faturanın alıcısına e-posta ile gönderilirken imzalı UBL ek olarak veya imzalı UBL'in özel entegratörün sistemlerinden indirilebileceği bir URL eposta ile birlikte gönderilmekte mi?	
K21	e-Arşiv Raporlarının gönderimleri özel entegratör üzerinden belirlenen terminlerde mi yapılmış?	
K22	Özel entegratör, müşteri firmanın düzenlenen her e-Arşiv Faturasının özel entegratör bilgi işlem sistemleri aracılığı ile oluşturup ve düzenlenen her e- Arşiv Faturasının GİB'e e-Arşiv Raporu ile raporlanmasını garanti edecek tedbirleri almış mı?	
4. Hizmetin Kapatılması		
K24	Hizmeti kapatmak isteyen müşteri için GİB'e kapatma isteği gönderilmekte mi?	
K25	Hizmeti kapatmak isteyen müşterilere e-Arşiv fatura / e-Arşiv Raporları UBL / GİB Rapor XML'i formatında teslim edilmekte mi?	

ÖEBSD_SIS.7: Hizmet Yazılımlarına İlişkin Kontroller		
e-İrsaliye		
Kontrol No	Kontrol Maddesi	Sonuç
1. Güvenlik		
L1	Her kullanıcı sadece kendi firması adına irsaliye gönderebilmekte mi?	
L2	Her kullanıcı sadece yetkisi olduğu firmanın alıcısı veya satıcısı olduğu irsaliyeleri görebilmekte mi?	

L3	Her kullanıcı sadece kendi firması adına irsaliye yanıtı gönderebilmekte mi?	
L4	Her kullanıcı sadece kendi firmasının alıcısı veya satıcısı olduğu irsaliyelere verilen irsaliye yanıtlarını görebilmekte mi?	
	2. İşlem Kayıtlarının Saklanması	
L5	Kullanıcıların yaptığı tüm işlemlerin kayıtları saklanmakta mı?	
L6	Kullanıcıların yaptığı tüm işlemleri içeren kayıtların değişmezliği sağlanmakta mı?	
	3. Standartlara Uyum	
L7	Web ara yüzünde veya web servis, SFTP vb. gibi çeşitli kanallarla müşterilerden alınan bilgilerle oluşturulan UBL irsaliyeler son halinde saklanmadan ve gönderilmeden önce GİB tarafından yayımlanan güncel şematron (schematron) kontrolünden geçirilmekte mi?	
L8	Özel entegratör tarafından imzalanmayıp farklı kanallardan imzalı olarak alınan irsaliyeler son halinde saklanmadan ve gönderilmeden önce imza kontrolünden geçirilmekte mi?	
L9	Özel entegratör tarafından imzalanan irsaliyeler imzalanırken GİB'in belirlediği standartlara uyarak imzalanmakta mı?	
L10	Özel entegratör tarafından imzalanan irsaliyeler imzalanırken imza sertifikasının geçerlilik süreleri kontrol edilmekte mi?	
L11	Özel entegratör tarafından imzalanan irsaliyeler imzalanırken imza sertifikasının geçerlilik süreleriyle CRL ve OCSP sonuçları kontrol edilmekte mi?	
L12	İrsaliye ve irsaliye yanıtlarının gönderimi için oluşturulan zarflar GİB'e gönderilemezse müşterilerin müdahalesine gerek kalmadan bir süre sonra yeniden denenmekte mi?	
L13	Gönderilen irsaliye veya irsaliye yanıtlarının zarf durum sorguları gönderim anından itibaren hemen ve sık sık yapılmamakta, sadece gönderim tarihinden itibaren 24 saat içinde GİB'den ve alıcıdan sistem yanıtı gelmeyen zarfların durumları GİB'den kontrol edilmekte ve en sık 5 saatte bir sorgulanmakta mı?	

L14	GİB tarafından iletilen zarflar hemen kontrol edilip işlenmemekte kaydedilip hemen dönülmekte, kontrol ve işleme daha sonra yapılmakta mı?	
L15	GİB tarafından iletilen zarflar kontrol edilip işlendikten sonra hatalı veya hatasız olarak sistem yanıtı dönülmekte mi?	
L16	Oluşturulan sistem yanıtlarının gönderilip gönderilemedikleri veya gönderildikten sonra başarıyla işlenip işlenemedikleri belirli aralıklarla sorgulanarak yeniden gönderilmekte mi?	
L17	Alınan zarflar kontrol edilirken GİB tarafından yayımlanan güncel şema kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
L18	Alınan zarflar kontrol edilirken GİB tarafından yayımlanan güncel şematron (schematron) kontrolleri yapılmakta ve geçersiz olanlar kabul edilmeyip hatayı gösteren sistem yanıtı dönülmekte mi?	
L19	Alınan zarflar kontrol edilirken irsaliye ve irsaliye yanıtları için imza olup olmadığı, varsa geçerli olup olmadığı kontrol edilmekte ve geçerli imzalar için geçerli, geçersiz imzalar için geçersiz şekilde sistem yanıtı dönülmekte mi?	
L20	Alınan irsaliye ve irsaliye yanıtları için oluşturulan sistem yanıtları sadece sistem tarafından otomatik olarak oluşturabilmekte, kullanıcıların web servis gibi yöntemlerle sistem yanıtı zarfları göndermesine izin verilmemekte mi?	
L21	Gelen irsaliyelere zarfın alınma zamanından itibaren 7 gün içinde irsaliye yanıtı oluşturulabilmekte daha sonra irsaliye yanıtı oluşturulamamakta mı?	
L22	Gelen irsaliyeler zarfın alınma zamanından itibaren 7 gün içinde irsaliye yanıtı gönderilebilmekte daha sonra irsaliye yanıtı gönderilmekte mi?	
L23	Gelen irsaliyelere irsaliye yanıtı oluşturulup oluşturulamayacağı kontrol edilirken irsaliyenin alındığı saat kontrol edilmemekte irsaliye yanıtının 7. günde 23:59'a kadar oluşturulmasına izin verilmekte mi?	
L24	Gelen irsaliyelere bir defa irsaliye yanıtı verildiğinde bir daha irsaliye yanıtı oluşturulmasına izin verilmemekte mi?	

L25	Gelen irsaliyelerin içindeki XSLT şablonlarındaki hatalar nedeniyle görüntülenemeyen irsaliyeler için GİB'in e-İrsaliye paketlerinde önerdiği gibi bir varsayılan XSLT irsaliye şablonu kullanılabilenekte, en azından irsaliye numarası, irsaliye tarihi, notlar gibi temel bilgilerin görüntülenmesi sağlanabilmekte mi?	
L26	Gönderilen irsaliyelere gelen irsaliye yanıtları alıcının gönderilen zarfa gönderdiği sistem yanıtının özel entegratör tarafından alınma zamanından 8 gün sonrasına kadar kabul edilmekte, daha sonra gelen irsaliye yanıtları kabul edilmemekte mi?	
L27	Gönderilen irsaliyeye daha önce irsaliye yanıtı geldiyse gelen irsaliye yanıtı kabul edilmemekte mi?	
L28	Gönderilen irsaliye ve irsaliye yanıtlarına GİB veya alıcı tarafından hatalı sistem yanıtı dönülmesi durumunda yeni irsaliye ve irsaliye yanıtı oluşturulması gerekmeyen durumlarda yeni irsaliye ve irsaliye yanıtı oluşturulması zorlanmadan mevcut irsaliye ve irsaliye yanıtı farklı bir zarfa konarak gönderilebilmekte mi?	
L29	Gönderilen irsaliye ve irsaliye yanıtlarının gönderim sonucu belirlenene kadar veya başarılı olduktan sonra yeniden başka bir zarfla gönderilmesine izin verilmemekte mi?	
L30	Özel entegratör, müşteri firmanın istemesi durumunda irsaliyelerini kendi mali mührüyle imzalamasına imkân sağlamakta mı?	
4. Hizmetin Kapatılması		
L31	Hizmeti kapatmak isteyen müşteri için GİB'e kapatma isteği gönderilmekte mi?	
L32	Hizmeti kapatmak isteyen müşterilere irsaliye ve irsaliye yanıtları UBL ya da zarf olarak XML formatında teslim edilmekte mi?	

EK 2. Denetçinin Görüşünü Oluşturması İçin Kılavuz

Denetçi, EK 1'de verilen 12 kontrol tablosunda yer alan toplam 208 kontrol maddesine göre denetim görüşünü oluşturacaktır. Görüşün oluşturulmasında, denetçinin uygulayacağı ilkeler aşağıda açıklanmıştır:

“Olumlu görüş” için, 208 kontrol maddesinin en az 166 maddesinin yanıtı “E” olmalı,

1. Maddede belirtilen koşul sağlanmış olsa dahi, herhangi bir değerlendirme sınıfından “E” yanıtlarının sayısı %70’in altında kalıyorsa “olumlu görüş” verilemez. %70 için hesaplanacak madde sayısı, o değerlendirme sınıfındaki toplam kontrol maddesinin %70’i tam sayıya karşılık gelmiyorsa, bulunan sayıdan küçük en büyük tamsayıdır.

“Olumlu görüş” verilememiş ise, verilecek görüş; “H”, “K” veya “G” cevaplarından sayısı fazla olana göre, sırasıyla “olumsuz”, “şartlı görüş” veya “görüşten kaçınma” kanaatine varılır.

Denetçi, kanaatinin oluşmasına dayanak bulgularını raporunda açıkça yazar. Bununla birlikte denetçi, bu Kılavuzda açıkça yazılmamış olsa dahi, her türlü görüş ve önerisine denetimin amacı ve kapsamına uygun olmak kaydıyla raporunda ayrıca yer verebilir.

EK 3. ÖEBSD Rapor Formatı

KAPAK DİZİN

DENETİM GÖRÜŞ YAZISI

EK 4’de yer alan şablonlara uygun biçimde denetim görüş yazısı burada yer alır. I- GENEL BİLGİ

Denetimin konusu ve kapsamı, denetim faaliyeti gerçekleştirilen özel entegratöre ilişkin tanımlayıcı bilgiler, denetim tarihleri, denetimin kapsadığı faaliyet dönemi ve denetim yapıldığı yer(ler) burada yazılır.

II- ÖEBSD DEĞERLENDİRMESİ

Denetim faaliyeti, kanıtları ve olguları içerecek biçimde burada açıklanır. EK 1’da yer alan tüm kontrollerin değerlendirmesi, ek belgeler, yorumlar ve açıklamalar ile EK 2’de yer alan kılavuza göre değerlendirme sonucuna nasıl ulaştığına bu bölümde yer verilir. Her değerlendirme sınıfı alt bileşeni ayrı bir başlık altında ele alınır. Bu Kılavuzda yer almayan veya yorumunda tereddüt duyulan bir hususla karşılaşılması halinde,

uluslararası kabul görmüş bilgi teknolojileri kontrol hedefleri sunan COBIT dokümanlarında yer alan usul ve esaslara göre yapılan değerlendirme de ayrı bir başlık altında burada açıklanır.

EK 4. Olumlu, Şartlı, Görüşten Kaçınma ve Olumsuz Görüş Yazısı Şablonları

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Olumlu Görüş

.....Yönetim Kuruluna / Yönetimine:

..... A.S.'nin/...../..... tarihi itibarıyla/...../..... tarih sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde/...../.....tarih ve sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve/...../..... Tarih vesayılı Resmi Gazete’de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, bütün önemli taraflarıyla,’nin/...../..... tarihi itibarıyla bilgi sistemleri süreçlerini üzerinde,/...../.....tarih ve sayılı Resmi Gazete’de yayımlanan ÖEBSD Hakkında Kılavuzunda belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Bas Denetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

Sorumlu Ortak Bas Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Şartlı Görüş

..... A.S. Yönetim Kuruluna:

..... A.S.'nin/...../..... tarihi itibarıyla/...../..... tarih sayılı Resmi Gazete'de

yayımlanan ÖEBSD Hakkında Kılavuz kapsamında bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde/...../.....tarih ve sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması A.S. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve/...../..... tarih vesayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Bağımsız denetim faaliyetine getirilen sınırlandırma ve bu nedenle denetlenemeyen süreçler, uygulamalar, kontroller; denetlenenin bilgi sistemleri süreçleri üzerinde tespit edilen önemli kontrol eksiklikleri ve bu kontrol eksikliklerinin denetlenenin bilgi sistemleri süreçlerinin bütününe veya büyük bir kısmını etkilememesine ilişkin görüşüne esas neden ve gerekçeler)

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, yukarıda (*....ncı paragrafta*) açıklanan *husus(lar)* nedeniyle, denetlenenin bilgi sistemleri üzerinde bu

hususun/hususların muhtemel etkileri haricinde bütün önemli taraflarıyla,
..... A.S.'nin

...../...../..... tarihi itibarıyla bilgi sistemleri süreçleri üzerinde,/...../.....tarih ve sayılı Resmi Gazete'de ÖEBSD Hakkında Kılavuzda belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmiştir.

Raporun Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Bas Denetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

Sorumlu Ortak Bas Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Olumsuz Görüş

..... A.S. Yönetim Kuruluna:

..... A.S.'nin/...../..... tarihi itibarıyla/...../..... tarih sayılı Resmi Gazete'de

yayımlanan ÖEBSD Hakkında Kılavuz kapsamında bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde/...../.....tarih ve sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması A.S. Yönetimi'nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve/...../..... Tarih vesayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz kapsamında belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu sistem ve süreçler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

[Doğal Kısıtlar]

Kontrollerin doğasında bulunan kısıtlamalar nedeniyle bilgi sistemleri süreçleri üzerinde kontrol zayıflıkları bulunabilir ve tespit edilemeyebilir. Bunun yanında, bulgularımıza dayanılarak elde edilen sonuçların gelecek dönemleri kapsayacak şekilde değerlendirilmemesi gerekmektedir. Mevcut şartların değişmesi, sistemlerde veya kontrollerde değişiklik yapılması veya kontrollerin etkinlik derecesinin bozulması gibi sebeplerden ötürü; bu sonuçların zaman içerisinde değişme riski bulunmaktadır.

(Denetlenenin bilgi sistemleri süreçleri üzerindeki kontrollerin etkin, yeterli ve uyumlu bulunmama Sebepleri)

[Bağımsız Denetçi Görüşü]

Görüşümüze göre, yukarıda (*...ncı paragrafta*) açıklanan *husus(lar)* nedeniyle,..... A.S.'nin

...../...../..... tarihi itibarıyla bilgi sistemleri süreçleri üzerinde,/...../.....tarih ve sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuzunda belirtilen usul ve esaslara uygun olarak etkin, yeterli ve uyumlu kontroller tesis edilmemiştir.

Raporun Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Bas Denetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

Sorumlu Ortak Bas Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

ÖZEL ENTEGRATÖRLER BİLGİ SİSTEMLERİ DENETİM RAPORU

Görüşten Kaçınma

..... A.S.'nin/...../..... tarihi itibarıyla/...../..... tarih sayılı Resmi Gazete'de yayımlanan ÖEBSD Hakkında Kılavuz bilgi sistemleri süreçlerini denetlemekle görevlendirilmiş bulunuyoruz.

[ÖE Yönetim Kurulunun Sorumluluğuna İlişkin Açıklama:]

Bilgi sistemleri süreçleri üzerindeki kontrollerin denetlenen nezdinde/...../.....tarih ve sayılı Resmi Gazete’de yayımlanan ÖEBSD Hakkında Kılavuzda belirtilen usul ve esaslara uygun olarak oluşturulmasının, etkin olarak işletilmesinin ve yeterli bir kontrol ortamı tesis edilmesinin sağlanması

..... A.S. Yönetimi’nin sorumluluğundadır.

[Yetkili Denetim Kuruluşunun Sorumluluğuna İlişkin Açıklama:]

Bağımsız denetimi yapan kuruluş olarak üzerimize düşen sorumluluk, yaptığımız denetim çalışmasına istinaden görüş bildirmektir. Yapmış olduğumuz denetim, denetlenenin bilgi sistemleri süreçleri üzerinde var olan önemli kontrol eksikliklerinin tespit edilmesine dair makul güvence sağlayacak şekilde planlanmış ve/...../..... tarih vesayılı Resmi Gazete’de yayımlanan ÖEBSD Hakkında Kılavuzda belirtilen usul ve esaslara uygun olarak gerçekleştirilmiştir. Denetim, bilgi sistemleri süreçleri ile bu süreç ve sistemler üzerindeki kontrollerin uyumluluk ile tasarım ve işletim etkinliğinin önemlilik ilkesi çerçevesinde test edilmesini, değerlendirilmesini ve ihtiyaç duyduğumuz ölçüde benzeri diğer denetim tekniklerinin uygulanmasını içermektedir.

Gerçekleştirilen denetimin, görüşümüzün oluşturulmasına makul ve yeterli bir dayanak oluşturduğuna inanıyoruz.

(Denetçinin görüş bildirmemesinin nedenleri) [Bağımsız Denetçi Görüşü]

Yukarıda (...ncı paragrafta) açıklanan husus(lar) nedeniyle A.S.’nin/...../.....

tarihi itibarıyla bilgi sistemleri süreçleri üzerinde tesis edilen kontrollerin etkinliği, yeterliliği ve uyumluluğu hakkında görüş bildirmiyoruz.

Raporun Düzenleme Yeri ve Tarihi

Sorumlu Bilgi Sistemleri Bas Denetçisinin Adı ve Soyadı, İmzası

Kuruluşun Ticari Unvanı

Sorumlu Ortak Bas Denetçinin Adı ve Soyadı, İmzası Kuruluşun Ticari Unvanı

EK 2. Çalışmanın Anketi

BAĞIMSIZ DENETÇİLERİN BİLGİ SİSTEMLERİ DENETİMİNİN BAĞIMSIZ DENETİME ETKİSİ KONUSUNDAKİ GÖRÜŞLERİ VE E-BELGE ÖZEL ENTEGRATÖRLERİ BİLGİ SİSTEM DENETİMİNE İLİŞKİN BİLGİ DÜZEYLERİNİN ARAŞTIRILMASI: ANKARA İLİ UYGULAMASI

Sayın Bağımsız Denetçi,

Bu anket çalışması, İnönü Üniversitesi, Sosyal Bilimler Enstitüsü, İşletme Anabilim Dalı'nda yapılan "Bilgi Sistemleri Denetiminin Bağımsız Denetime Etkisi: E-Belge Özel Entegratör Kuruluşları Üzerine Bir Araştırma" doktora tez çalışmasıyla ilgilidir. Ankette yer alan sorular tamamen akademik ve bilimsel amaçlara yönelik olarak kullanılacak ve vereceğiniz cevaplar kesinlikle gizli tutulacaktır.

Anket formunun üzerine adınızı ve soyadınızı yazmayınız. Cevaplarınız sadece bilimsel amaçlıdır ve gizli tutulacaktır. Bu bağlamda anketin güvenilirliğinin, tarafsızlığının ve amacına ulaşmasının sağlanması için lütfen soruları dikkatlice cevaplayınız. Desteğiniz ve araştırmamıza yapacağınız önemli katkılarınızdan dolayı şimdiden çok teşekkür ederiz.

Zeliha KOCA
Doktora Öğrencisi
İnönü Üniversitesi
Sosyal Bilimler Enstitüsü
İşletme Anabilim Dalı
Muhasebe Finansman Bilim Dalı

Doç. Dr. Ahmet Fethi DURMUŞ
Tez Danışmanı
İnönü Üniversitesi
İktisadi ve İdari Bilimler Fakültesi
İşletme Bölümü

BİRİNCİ BÖLÜM

- 1. Cinsiyetiniz** Erkek () Kadın ()
- 2. Yaşınız** 30 ve Altı () 30-39 () 40-49 () 50-59 () 60 ve Üzeri ()
- 3. Öğrenim Durumunuz** Lisans () Yüksek Lisans () Doktora ()
- 4. Bağımsız Denetçi Olarak Çalışma Süreniz** 1-5 yıl () 6-10 yıl () 11-15 yıl () 16 yıl ve üzeri ()
- 5. Denetim Firmasındaki Pozisyonunuz** Denetçi Yardımcısı () Denetçi () Kıdemli Denetçi () Baş Denetçi () Sorumlu Ortak Baş Denetçi ()

6. e- Belge Özel Entegratör kuruluşları hakkında bilgi sahibi misiniz? Evet () Kısmen () Hayır ()
7. E- Fatura, E-Defter, E-Arşiv hakkında bilgi sahibi misiniz? Evet () Kısmen () Hayır ()
8. Bilgi sistemleri Denetim ve Kontrol Birliği (ISACA) tarafından verilen bilgi sistemleri denetçisi sertifikası (CISA)'na sahip misiniz?
Evet () Hayır ()
9. Aşağıda yer alan ERP/Muhasebe Yazılım Program'larından hangisi hakkında bilgi sahibisiniz. (Diğeri seçtiyseniz ne olduğunu yazınız)
- SAP () Logo () Eta () Netsis () Mikro () Zirve () Luca () Diğer ()

İKİNCİ BÖLÜM

Lütfen Aşağıda Yer Alan Bilgi Sistemleri Denetimi ve Bağımsız Denetim ile İlgili İfadelere Katılma Düzeyinizi Belirtiniz.	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1. Bilgi sistemleri denetimi bağımsız denetimin bir parçasıdır, bağımsız denetim süreci içinde kapsamlı şekilde incelenmesi ve analiz edilmesi gerekir.					
2. Bilgi sistemleri denetimi, bağımsız denetçinin muhasebe ve iç kontrol sistemi ile ilgili yeterli bir anlayış edinmek amacıyla izlediği yöntemleri etkilemez.					
3. Bağımsız denetimde bilgi sistemlerinin üzerinde durulmaması denetimin güvenilirliğini yani denetimin gerçekleştirilme amacı olan makul güvenceyi zedeler.					
4. Bilgi sistemlerindeki donanım ve yazılım hatalarının bağımsız denetim üzerinde olumsuz etkisi vardır.					
5. Bilgi sistemleri denetimi ile uyum içerisinde yürütülen denetim çalışması daha şeffaf sonuçların ortaya konmasına katkı sağlayacaktır.					
6. Bilgi sistemlerindeki altyapı yetersizlikleri ve performans sorunlarının bağımsız denetim üzerine etkisi vardır.					
7. Bilgi sistemleri kontrol ve denetim faaliyetlerinin yetersizliğinin bağımsız denetime etkisi yoktur.					
8. Bilgi sistemlerindeki veri ve programlara yetkisiz erişimin bağımsız denetim üzerinde etkisi yoktur.					
9. Denetim planı oluşturulurken, denetim riskinin büyüklüğü belirlenirken bilgi sistem denetimi sonuçları dikkate alınmalıdır.					
10. Bilgi sistemleri denetimin de iç kontrol ve denetim mekanizmaları değerlendirmelerinin bağımsız denetim kanıt güvenilirliğine etkisi vardır.					
11. Bilgi sistemleri denetimi şirket verilerine erişimi sınırlayarak yasalara ve muhasebe standartlarına uyumu geliştirir, kontrolleri iyileştirir.					
12. Bilgi sistemleri üzerine siber saldırıların bağımsız denetim üzerinde olumsuz etkisi vardır.					

13. Bilgi sistemlerinin söz konusu verileri doğru üretip üretmediği bağımsız denetim çalışmasının doğruluğuna ve bütünlüğüne doğrudan etki etmez.					
14. Bağımsız denetçi, bilgi sistemlerinin içyapısında bulunan önemli olarak değerlendirilebilecek hata ve yanlışlıkların denetim sonuçlarına etkilerini açıklamalıdır.					
15. Finansal tablolara kaynak verilerin doğru bir şekilde sisteme girilip girilmediği, sistem içinde işlenirken bozulmaya uğrayıp uğramadığı ve söz konusu verilerin yetkili kişiler tarafından yönetilip yönetilmediği incelenmelidir.					
16. Bilgi Sistemleri Denetimi üzerine bağımsız denetçilere zorunlu eğitim verilmelidir.					

ÜÇÜNCÜ BÖLÜM

Özel entegratörler, GİB'in belirlediği belirli koşulları karşılayarak mükellef adına birçok **e-Dönüşüm hizmeti** için elektronik kayıt (e-defter, e-fatura v.b) oluşturma yetkisine sahip aracı kurumlardır.

Lütfen Aşağıda Yer Alan e- Belge Özel Entegratör Bilgi Sistem Denetimi ile İlgili İfadelere Katılma Düzeyinizi Belirtiniz. 1= Kesinlikle Katılmıyorum 2= Katılmıyorum 3= Kararsızım 4= Katılıyorum 5= Kesinlikle Katılıyorum	Kesinlikle Katılmıyorum	Katılmıyorum	Kararsızım	Katılıyorum	Kesinlikle Katılıyorum
1. Uluslararası standartlara ilişkin güncel sertifikasyonlara sahip olmak bilgi sistemleri kalitesini etkiler.					
2. Sızma testlerinin güncellenmesi, saldırı yöntemlerine göre test edilmesi bilgi güvenliğini etkiler.					
3. Sızma testlerinin kalitesi ya da sayısı bilgi sistemleri kalitesini etkilemez.					
4. GİB tarafından saklama hizmeti verme izni almış firmanın, mükellefin e-Belge uygulamaları kapsamında oluşturulan belgelerinin BİS raporuna uygun olarak saklanması bilgi sistemleri kalitesini artırır.					
5. İç kontrol ve iç denetim dokümanı oluşturulması bilgi sistemleri kalitesini etkilemez.					
6. İç kontrol dokümanları ile iş sürekliliği belgelerinin birbiriyle uyumlu olması bilgi sistemleri kalitesini etkiler.					
7. İç kontrol denetimlerinin periyodik biçimde yapılması ve denetim sonuçlarının raporlanması bilgi sistemleri kalitesini etkilemez.					
8. İstihdam edilen personelin öğrenimi ve sertifikasyonlarının göreviyle uygun olması bilgi sistemleri kalitesini etkilemez.					
9. Sistemlerin yönetiminde, veri tabanı ve uygulamaların geliştirilmesinde, test edilmesinde ve işletilmesinde görev ve sorumlulukların ayrılığı prensibinin uygulanması bilgi sistemleri kalitesini artırır.					
10. Uygun nitelik ve sayıda personel istihdamı bilgi sistemleri kalitesini artırmaz.					
11. Özel Entegratör yönetici ve çalışanlarının kamusal bir görev ifa ettiklerinin bilinci ile hareket etmeleri bilgi sistemleri kalitesini artırır.					
12. Hassas verilerin (mükellef bilgileri, erişim şifreleri vb.) veri tabanında şifreli saklanması bilgi sistemleri kalitesini artırır.					
13. Veri tabanı, uygulama ve ağ erişim cihazları (güvenlik duvarı, aktif anahtarlama cihazları) katmanlarında tek noktadan arıza sonucu hizmetin					

durmasına izin verecek bir yapılanma olmadığının kontrol edilmesi bilgi sistemleri kalitesini artırır.					
14. Sunucuların veya aktif ağ cihazlarının yer aldığı sistem odaları ile kritik odalar, iklimlendirme, güç şebekesi, sel, yangın ve benzeri afetler için otomatik uyarı ve söndürme sistemleri gibi fiziksel altyapı gerekliliklerinin sağlanması bilgi sistemleri kalitesini artırmaz.					
15. Hassas verilere herhangi bir personelin tek başına erişim yetkisinin olmaması bilgi sistemleri kalitesini artırmaz.					
16.Sistem odaları ve kritik odalara erişim yetkilendirmeleri ve değişikliklere ilişkin kayıtların güvenli biçimde tutuluyor olması bilgi sistemleri kalitesini artırır.					
17. Tek yönetici erişimiyle veri ve uygulama değişikliği yapılmasını engelleyecek mekanizmalar kurulmuş olması bilgi sistemleri kalitesini artırmaz.					
18. Özel entegratörün, bir risk yönetim planı oluşturması bilgi sistemleri kalitesini artırır.					
19. Donanımlara, yazılımlara, uygulama geliştirme faaliyetine, iletişim alt yapılarına ve dış hizmet alımlarına bağlı olayların risk yönetim planına dâhil edilmesi bilgi sistemleri kalitesini artırmaz.					
20. Bilgi sistemlerinin belirlenen süreleri aşan biçimde hizmet veremez hale gelmesi durumunda yapılacaklar için bir acil durum planı hazırlanması bilgi sistemleri kalitesini artırmaz.					
21. Özel entegratörün, bilgi sistemlerinde kullandığı her türlü sunucu, veri tabanı, güvenlik duvarı, aktif ağ cihazı ve işletim sistemi kayıtları ile mükellef ve GİB ile haberleşmesinde kullanılan yazılım uygulamalarının veri tabanı motorları ve uygulama kayıtlarını tutması (denetim izi) bilgi sistemleri kalitesini artırır.					
22.Denetim izlerinin bütünlüğünün korunması ve tahrifatı halinde bunun tespiti için yeterli tedbirler alınması bilgi sistemleri kalitesini artırmaz.					
23.Denetim İzleri yönetimi için veri tabanı katmanı, uygulama katmanı, ağ cihazları ile işletim sistemleri için denetim izlerinin nasıl oluştuğunun ve saklandığının kayıt altına alınmış olması bilgi sistemleri kalitesini artırır.					
24. Değişiklik yönetimi prosedüründe, bilgi sistemlerinde yer alan tüm donanım ve yazılımın her türlü bakım, yama ve değişikliğinin kapsamda yer alması bilgi sistemleri kalitesini artırır.					
25. Özel entegratörün, hizmetlerinde kullandığı, mükellef ve GİB ile entegrasyonu sağlayan yazılımların değişiklik yönetimini yapması bilgi sistemleri kalitesini artırır.					
26.Değişiklik yönetimi için bir prosedür oluşturulması bilgi sistemleri kalitesini artırır.					
27. Özel entegratörün, dış hizmet sağlayıcısını iç kontrol ve denetim prosedürleri uyarınca düzenli aralıklarla denetlemesi bilgi sistemleri kalitesini artırır.					
28. Kullanıcıların yaptığı tüm işlemlerin kayıtlarının saklanması bilgi sistemleri kalitesini artırmaz.					
29.Özel entegratörün dış hizmet alımını sözleşmeye dayalı yapması bilgi sistemleri kalitesini artırır.					
30. Her kullanıcının sadece yetkisi olduğu firma adına fatura gönderebilmesi bilgi sistemleri kalitesini artırır.					
31. Düzenlenen her e-Fatura ve uygulama yanıtında yer alan bilgilerin gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırmaz.					
32. Düzenlenen her e-Arşiv Fatura, e-SMM, e-MM, e-Bilet vb. altyapıda işleyen elektronik belgeler ve oluşturulan her e-Arşiv raporunda yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.					

33. Düzenlenen her e-İrsaliye ve irsaliye yanıtında yer alan bilgilerin tamamının gizliliği ve bütünlüğünün korunması bilgi sistemleri kalitesini artırır.

--	--	--	--	--

