

## Bilgi Teknolojileri Yönetişiminin Denetimi

Kaan Ramazan ÇAKALI<sup>1</sup>

Gürol BALOĞLU<sup>2</sup>

### Özet

Bilgi teknolojileri süreçleri işletmelerin faaliyetlerinde kritik rol oynamaktadır. Bilgi teknolojileri yönetişiminin sağlanması, işletmelerin kritik başarı faktörlerinin başında gelmektedir. Bilgi teknolojileri yönetişimi, iş gereksinimleriyle bilgi teknolojileri operasyonlarının birbirleriyle uyum içerisinde olmasını sağlar. Bilgi teknolojileri denetimlerinin temel amacı bilgi teknolojileri süreçlerine yönelik kontrollerin etkinliği ve yeterliliğinin iç denetim birimlerince değerlendirilmesidir. Bilgi teknolojileri denetimleri kapsamında gerçekleştirilen en önemli çalışmaların başında bilgi teknolojileri yönetim çerçevesinin ve süreçlerinin gözden geçirilmesi gelmektedir. Bu çalışmanın amacı, bilgi teknolojileri yönetişimi alanında verilecek güvence hizmetlerine yönelik olarak bir kapsam önerisinde bulunulması olarak belirlenmiştir. Bu amaçla, nitel araştırma yöntemlerinden doküman analizi yönteminden faydalanılmak suretiyle işletmelerde bilgi teknolojileri yönetim yapılarına yönelik gerçekleştirilecek iç denetim çalışmalarında dikkate alınması gereken inceleme alanları belirlenerek bir kapsam önerisinde bulunulmuştur.

**Anahtar Kelimeler:** İç Denetim, Güvence Hizmetleri, Bilgi Teknolojileri, Bilgi Teknolojileri Yönetişimi, Bilgi Teknolojileri Yönetişimi Denetimi

## Auditing Information Technology Governance

### Abstract

Information technology processes play a critical role in the activities of businesses. Ensuring information technology governance is one of the critical success factors of enterprises. Information technology governance ensures that business requirements and information technology operations are in a harmony with each other. The main purpose of information technology audits is to evaluate the effectiveness and adequacy of controls on information technology processes by internal audit units. The most important work carried out within the scope of IT audits is the review of the IT governance framework and processes. The aim of this study is to propose a scope for assurance services to be provided in the field of information technology governance. For this purpose, by making use of the document analysis method, one of the qualitative research methods, a scope proposal has been made by determining the areas of investigation that should be taken into account in the internal audit engagements to be carried out for the information technology governance structures in the enterprises.

**Keywords:** Internal Audit, Assurance Services, Information Technology, Information Technology Governance, Auditing Information Technology Governance

### Derleme Makale / Review Article

Makale Geliş Tarihi / Submitted: 21.10.2021 Makale Kabul Tarihi / Accepted: 5.1.2022

<sup>1</sup> Sorumlu Yazar, Dr., Türkiye Kalkınma Yatırım Bankası A.Ş., Teftiş Kurulu Başkanı, İstanbul/Türkiye, kaanramazanc@gmail.com, ORCID ID: 0000-0003-4186-2291

<sup>2</sup> Dr., Süzer Grubu, Denetim Grubu Başkanı, İstanbul/Türkiye, gurol@live.com, ORCID ID: 0000-0003-1093-2664

**Atf (Citation):** Çakalı, R., K. ve Baloğlu, G. (2022). Bilgi teknolojileri yönetişiminin denetimi. *Denetim ve Güvence Hizmetleri Dergisi* 2(1), 1-13.

## 1. GİRİŞ

Son yıllarda bilgi teknolojileri alanında yaşanan gelişmeler, şirket faaliyetlerinin bilgisayar ortamında gerçekleşmesi, bilgi teknolojilerine yönelik sistemlerin kullanımının hızla yayılması gibi sebeplerden ötürü bilgi teknolojileri kaynaklı riskler hayatımıza daha fazla girmeye başlamıştır. Bu risklerin tanımlanması, değerlendirilmesi ve işletmeleri maruz bırakacak etkilerinin azaltılmasına yönelik aksiyonların alınması önemli hale gelmiştir.

Dünyada, bilgi teknolojileri kapsamında yapılan yatırımların miktarı gün geçtikçe artmakta ve işletmeler bilgi teknolojilerine daha fazla bağımlı hale gelmektedirler. Bu değişim ve gelişim dünyada tüm sistemlerin yanı sıra iç denetim faaliyetlerinin de değişimine ve odak noktasını tekrar gözden geçirme ihtiyacının doğmasına sebep olmuştur. İşletmeler bünyesinde bilgi teknolojileri denetim ekipleri kurulmaya başlanmış ve bilgi teknolojileri kaynaklı risklerin etkin yönetimi şirketlerin öncelikli konuları arasına girmiştir.

Bilgi teknolojilerinin artan önemine paralel bir şekilde bilgi teknolojileri yönetişimi kavramı da hayatımıza girmiştir. En genel tanımıyla bilgi teknolojileri yönetişimi, işletmelerin bilgi teknolojileri yapılarının kurumların hedefleriyle paralel hale getirilmesi suretiyle kaynakların etkin kontrol edilmesi sürecidir. Bilgi teknolojileri yönetişiminin önemi ile birlikte işletmelerde bu sürecin iç denetim birimlerince gözden geçirilmesi hususu da iç denetim birimlerinin öncelikli görevleri arasında yer almaya başlamıştır.

Bu çalışmanın temel amacı, bilgi teknolojileri yönetişimi alanında gerçekleştirilecek denetim çalışmalarında kullanılmak üzere bir kapsam önerisinde bulunulması olarak belirlenmiştir. Çalışmada, nitel araştırma yöntemlerinden doküman analizi yönteminden faydalanılmıştır (Aydın, 2018: 61). Çalışmanın ilk bölümünde bilgi teknolojileri yönetişim süreçlerinin denetimine yönelik literatür taramasına yer verilmiştir. Sonrasında, iç denetim ve bilgi teknolojileri denetimi kavramları açıklanmıştır. Takip eden bölümlerde bilgi teknolojileri yönetişimine ilişkin detaylı bilgilere yer verilmiş ve uygulama bölümünde bu sürecin iç denetiminin gerçekleştirilmesi esnasında odaklanılması gereken riskler ve alanlar tanımlanmıştır. Son olarak, sonuç bölümüyle çalışma tamamlanmıştır.

## 2. İÇ DENETİM VE BİLGİ TEKNOLOJİLERİ DENETİMİ

İç denetim, işletmelerin bünyelerinde çalışan iç denetim personeli tarafından gerçekleştirilen ve kurumun faaliyetlerini geliştirmeyi amaçlayan bağımsız güvence ve danışmanlık faaliyeti olarak tanımlanabilir. İç denetim, disiplinli ve sistematik bir bakış açısıyla gerçekleştirdiği çalışmalarla kurumun hedeflerine ulaşmasına destek olmaktadır. Bu faaliyet çerçevesinde, işletmelerin kurumsal yönetim, kontrol ve risk yönetimi süreçleri değerlendirilmekte ve bu süreçlerde mevcut olan kontrollerin etkinliği ve yeterliliği konusunda değerlendirme ve tavsiyelerde bulunmaktadır (IIA, 2019: 242).

İç denetimin yukarıda yer verilen ve IIA tarafından yapılan genel kabul görmüş tanımına bakıldığında aşağıda belirtilen temel unsurların öne çıktığı görülmektedir (IIA, 2019: 242):

- İç denetim, işletmelere değer katma amacını gütmektedir.
- Güvence ve danışmanlık hizmetleri olmak üzere iki temel hizmet türü bulunmaktadır.
- Bağımsız ve tarafsız bir faaliyettir.
- Süreçlerdeki kontrollerin etkinliği ve yeterliliği üzerine odaklanmaktadır.
- Bu faaliyet kapsamında işletmelerin kurumsal yönetim, risk yönetimi ve kontrol süreçlerinin gözden geçirilmesi sağlanmaktadır.
- İç denetim faaliyeti kapsamında gerçekleştirilen çalışmalar sonucunda değerlendirme ve önerilerde bulunulur.

İç denetim faaliyetlerinin işletmelere sağladığı faydalar değerlendirildiğinde ise temel olarak aşağıda belirtilen hususların öne çıktığı görülmektedir (Celayir, 2021: 70):

- İşletme içerisinde üretilen bilgilerin güvenilirliğinin sağlanması,
  - Kurumun fiziki varlıklarının ve muhasebe kayıtlarının korunması,
-

- İşletmenin faaliyetlerini verimli bir şekilde sürdürmesine yönelik katkı sağlanması,
- Kurum bünyesinde düzenlenmiş olan politika ve prosedürlere uyumun sağlanması.

İç denetim faaliyetleri kapsamında gerçekleştirilen en önemli çalışmaların başında bilgi teknolojileri süreçlerinin denetimi gelmektedir. Bilgi teknolojileri denetimleri, işletmelerin tüm teknolojik altyapılarının, güvenlik, yazılım ve donanım gibi hususlarının risk odaklı bir bakış açısıyla gözden geçirilmesi olarak tanımlanabilir. Bilgi teknolojileri kapsamında iki tür kontrolden bahsedilebilir. Bunlar; genel bilgi teknolojileri kontrolleri ve uygulama kontrolleridir. Bilgi teknolojileri denetimlerinin temel amacı bahsedilen kontrollerin etkinliğine ve yeterliliğine yönelik güvence verilmesidir (Özbek, 2012: 152).

Bilgi teknolojileri denetimleri kapsamında, iç denetim birimlerince kurumlarında bilgi teknolojilerine ilişkin süreçlerdeki kontrollerin etkinlik ve yeterliliklerinin değerlendirilmesi ve bilgi teknolojileri risklerinin etkin yönetilmesine yönelik güvence ve danışmanlık faaliyetleri gerçekleştirilmektedir.

İç denetim mesleğine yönelik olarak IIA tarafından hazırlanan uluslararası iç denetim standartları kapsamında da iç denetçilere, kurumlarının bilgi teknolojileri süreçlerinde gerçekleştirmeleri gereken çalışmalara yönelik bir takım yükümlülükler getirilmektedir. Standartlar incelendiğinde, iç denetçilerin bu yöndeki sorumluluklarına ilişkin olarak, standartların yönetim, risk yönetimi ve kontrol başlıkları altında aşağıdaki hususların öne çıktığı görülmektedir (IIA, 2019):

- İç denetim birimlerinin işletmelerindeki bilgi teknolojileri yönetişiminin işletmenin hedef ve stratejilerini desteklediğine yönelik değerlendirmelerde bulunmaları gerekmektedir.
- İç denetim birimleri, işletmenin maruz kaldığı bilgi teknolojilerine yönelik risklerin değerlendirilmesinden sorumludur.
- İç denetim çalışmalarının, bilgi teknolojileri risklerine cevap olarak, işletme bünyesindeki kontrollerin etkinliği ve yeterliliğinin değerlendirmesi gerekmektedir.

### 3. BİLGİ TEKNOLOJİLERİ YÖNETİŞİMİ

Bilgi teknolojileri yönetişi, işletmelerin bilgi teknolojilerine yönelik yapılarının kurum hedef ve stratejilerini desteklemesine katkı sağlayan kurumsal yapı, liderlik ve ilgili süreçlerinden meydana gelmektedir (IIA, 2019: 240). Bilgi teknolojileri yönetişi, teknoloji ve kaynakların kullanılması suretiyle tanımlanan organizasyon yapılarının bilgi teknolojileri kaynaklarını kontrol etmelerine yönelik tasarlanan süreçtir (Hunton, Bryant ve Bagranoff, 2004: 2). İşletmelerin yönetim kurullarının ve üst yönetim kadrolarının iş süreçleri ile bilgi teknolojilerine ilişkin süreçlerin birbirleriyle entegre olmalarını sağlayacak stratejinin planlanması ve uygulanması olarak da tanımlanabilir (De Haes ve Van Grembergen, 2004: 1).

Yapılan tanımlar dikkate alındığında bilgi teknolojileri yönetişimine ilişkin olarak aşağıda belirtilen hususların öne çıktığı görülmektedir (Kayrak, 2013: 59):

- Bilgi teknolojileri yönetişi kurumsal yönetişimin bir alt dalıdır.
- İşletmeler bünyesinde bilgi teknolojileri yönetim süreçlerine yönelik nihai sorumluluk yönetim kurullarındadır.
- İşletme personeli, kendi görev tanımları çerçevesinde bilgi teknolojileri yönetim süreçlerine destek olurlar.
- Bilgi teknolojileri yönetişi, bilgi teknolojileri yönetiminden farklı bir kavram olarak karşımıza çıkmaktadır.
- Bilgi teknolojileri yönetişi, süreç, kurumsal yapı ve liderlik fonksiyonlarından oluşmaktadır.
- Bilgi teknolojileri yönetişi, etkinlik, verimlilik ve tutumluluğu ön planda tutmaktadır.

Bilgi teknolojileri yönetişiminin amacı, aşağıda belirtilen hedeflerin gerçekleşmesine yönelik olarak bilgi teknolojileri çabalarının yönlendirilmesidir (ITGI, 2007: 3):

- İşletme ile bilgi teknolojilerinin uyumlu hale getirilmesi ve beklenen faydaların gerçekleşmesi,
- Bilgi teknolojilerinin fırsatlardan yararlanmak ve en üst seviyede fayda elde etmek amacıyla kullanımı,
- Kaynakların sorumlu kullanımı,
- İşletme bünyesindeki bilgi teknolojileri kaynaklı risklerin etkin yönetimi.

Bilgi teknolojileri yönetiřimi, kurumun bilgi teknolojileri varlıklarının ve risklerinin gözetimiyle ilgilidir. Bu sorumluluk ise řletmelerin yönetim kurulu ve üst yönetimlerindedir. Etkin işleyen bilgi teknolojileri yönetiřim süreçleri řletmeler bünyesinde aşağıda belirtilen hususların gerçekteşmesine katkı sağlayacaktır (IIA, 2018: 4):

- Kurumsal hedeflerle bilgi teknolojileri stratejilerinin birbirleriyle ilişkili olması,
- Risklerin sağlıklı bir şekilde tanımlanıp yönetilmesinin sağlanması,
- Bilgi teknolojilerine yönelik yatırımların optimize edilmesi,
- Bilgi teknolojileri performansının ölçümü,
- Bilgi teknolojileri kaynaklarının etkin ve verimli kullanımı.

Bilgi teknolojileri yönetiřimi, hedeflerine ulaşma yönünde aşağıda belirtilen 5 temel alanla ilgilenmektedir (ITGI, 2003: 19):

- Stratejik uyum
- Deęer sağlama
- Risk yönetimi
- Kaynak yönetimi
- Performans ölçümü

Bu alanların her birine yönelik açıklamalara aşağıda yer verilmektedir.

### 3.1. Stratejik Uyum

Stratejik uyum, temel olarak resmi iş hedefleri ile güncel bilgi teknolojileri stratejisinin mevcudiyeti ile işletme hedefleriyle bilgi teknolojileri stratejilerinin paralel olmasına odaklanmaktadır (Iliescu, 2010: 95). Bir işletmenin bilgi teknolojilerine yönelik yapmış olduęu yatırımlarının mevcut kurumsal hedefleri ve stratejileriyle uyumlu olup olmadığının belirlenmesidir. Buradaki temel konu, bilgi teknolojileri stratejisinin işletme stratejisini desteklemesidir. Bu durum, kurumsal hedeflerin sıklıkla deęiřmesi sebebiyle her zaman elde edilememektedir. Ancak, yine de odaklanması gereken bir konudur. Bu sebeple, bilgi teknolojileri stratejilerinin oluşturulması aşamasında aşağıdaki hususların dikkate alınması gereklidir (ITGI, 2003: 22-23):

- İşletme hedefleri ve rekabet ortamı,
- Mevcut ve gelecek teknolojiler ile bunların kuruma sağlayacağı faydalar ve işletmeyi maruz bırakabilecekleri riskler ve maliyetleri,
- İşletmenin bilgi teknolojileri organizasyon ve yapısının mevcut durumda ve gelecekte kuruma gereken hizmeti sağlayabilme yeteneęi,
- Bilgi teknolojileri maliyetinin işletmeye sağladığı deęer açısından deęerlendirilmesi,
- Geçmiş dönemlerde yaşanan olumsuz örneklerden alınan dersler.

İşletmenin yönetim kurulu veya bilgi teknolojileri strateji komitesi tarafından aşağıdaki hususların yerine getirilmesi suretiyle stratejik uyum sağlanabilecektir (ITGI, 2003: 23-24):

- Dağıtılmış bilgi teknolojileri stratejilerinin bütünleşmiş ve iş stratejileriyle uyumlu olmasının sağlanması,
- Net beklenti ve ölçüm mekanizmalarının oluşturulması,
- Kurumu destekleyen ve rekabet etmesini sağlayan bir altyapı oluşturan sistemlerin arasındaki yatırımların dengelenmesinin sağlanması,
- Bilgi teknolojileri kaynaklarının odak noktalarına yönelik olarak düşünölmüş kararların alınması.

Stratejik uyumla ilgili temel bilgi teknolojileri süreçleri; risk yönetimi, bütçe yönetimi, bilgi teknolojileri mimarisi, izleme, yasal ve stratejik uyum olarak sıralanabilir (Kayrak, 2013: 69).

### 3.2. Deęer Sağlama

Bilgi teknolojileri deęerinin temel ilkeleri uygun kalitenin bütçe dâhilinde ve planlanan zamanda teslim edilmesidir. İş terminolojisi açısından bakıldığında bu durum, rekabet avantajı, hizmetin sağlanması yönünde geçen zaman dilimi, müşteri bekleme süresi, memnuniyet ve kârlılık olarak nitelendirilebilir. Etkili bilgi

teknolojileri değerinin elde edilebilmesi için gerçek maliyetler ve yatırım getirisi birlikte yönetilmelidir (ITGI, 2003: 24).

İş sürekliliği, donanım ve yazılım alımı ve bakımı, organizasyon yönetimi, risk yönetimi, maliyet yönetimi, üçüncü taraflarla ilişkilerin yönetimi, personel yönetimi, izleme ve eğitim değer sağlamayla ilişkili temel süreçler olarak sıralanabilir (Kayrak, 2013: 70).

Bilgi teknolojilerinin bir kuruma kattığı değer, organizasyonel yapısının işletme ile ne ölçüde uyumlu olduğu ve kurumun beklentilerini karşılama seviyesi ile ilişkilidir. İşletmeler, bilgi teknolojileri çıktılarının içeriğine yönelik aşağıdaki hususları belirlemelidirler (ITGI, 2003: 25):

- Amaca uygun bir şekilde iş gereksinimlerini karşılması,
- Gelecekteki gereksinimleri karşılayabilecek esnekliğe sahip olması,
- Yanıt süreleri,
- Güvenlik, esneklik ve kullanım kolaylığı,
- Bilgi güncelliği, bütünlük ve doğruluğu.

### 3.3. Risk Yönetimi

Risk yönetimi, işletmelerin hedeflerine ulaşmaları yönünde karşılaşılabilecekleri potansiyel olumsuz olayların tanımlanması, analiz edilmesi ve kontrol altına alınması aşamalarını içeren bir süreçtir (IIA, 2019: 244). Etkin bir risk yönetimi süreci, işletmenin risk iştahının belirlenmesi ve yüksek düzeydeki risk maruziyetlerinin anlaşılması ile başlamaktadır. Sonrasında risk yönetimine yönelik stratejiler ve sorumluluklar belirlenir. Belirlenen risklerin türüne ve önem düzeyine göre, risklerin indirgenmesi, transfer edilmesi veya kabul edilmesine yönelik aksiyonlar alınır (ITGI, 2003: 27). Risk yönetimine yönelik sorumlulukların belirlenmesi, risk analiz yöntemlerinin tanımlanması ve sürekli izleme mekanizmalarının tesis edilmesi gereklidir (Iliescu, 2010: 95).

### 3.4. Kaynak Yönetimi

Bilgi teknolojilerinin performansının başarılı olmasının en temel kriterleri kaynakların optimal bir şekilde yatırımı, kullanımı ve tahsis edilmesi olarak sıralanabilir. İşletmelerin önemli bir kısmı, bilgi teknolojileri varlıklarının verimliliğini yükseltmekte ve bunlarla ilgili maliyetlerini en düşük seviyede tutmakta zorlanmaktadır. Şirket yönetim kurulları aşağıda belirtilen hususları sağlamak suretiyle uygun yatırımları ele almalıdırlar (ITGI, 2003: 28):

- Bilgi teknolojileri satın almalarına yönelik sorumlulukların belirlenip uygulanması,
- Bilgi teknolojileri sistemlerinin yönetimi ve desteklenmesi çerçevesinde uygun metod ve yeterli düzeyde etkinliklerin mevcut olması,
- Bilgi teknolojileri çalışanlarının işe alım ve elde tutulması süreçlerine yönelik işgücü planlama ve yatırımlarının bulunması,
- Bilgi teknolojilerine yönelik eğitim ihtiyaçlarının belirlenmesi,
- Çalışanların gerekli becerilerini geliştirmelerine yönelik uygun zemin ve zamanın sağlanması.

Bilgi teknolojileri kaynak yönetimine ilişkin temel süreçler; kapasite yönetimi, veri yönetimi, bilgi teknolojilerine yönelik insan kaynağının yönetimi, operasyonların yönetimi, altyapı alımı ve bakımı ve maliyet yönetimi olarak sıralanabilir (Kayrak, 2013: 71).

### 3.5. Performans Ölçümü

Bilgi teknolojileri performans ölçümü, bilgi teknolojileri faaliyetlerinin işletmeye kattığı değer ve bilgi teknolojileri hedeflerinin gerçekleşme durumunun belirlenmesine yardımcı olur. Performans ölçümü sayesinde işletme hedefleri ile bilgi teknolojileri hedeflerinin uyumlu olmasına katkı sağlar (NCC, 2005: 9-10).

İşletme yöneticileri, dengeli puan kartlarını kullanmak suretiyle kurumların kısa vadeli finansal sonuçlarından daha fazlasını dikkate alırlar. Ayrıca, müşteri memnuniyeti, operasyonel verimliliğin sağlanması, personelin gelişimi ve iç süreçlerin düzenlenmesi gibi hususlar dikkate alınmaktadır. Bu şekilde gerçekleştirilen bütünsel

---

yaklaşım sayesinde kısa vadeli faaliyetler ile uzun vadeli hedefler arasında bağlantı kurulması sağlanmaktadır (ITGI, 2003: 29).

Performans ölçümü, sürekli izleme ve raporlama, takip süreçleri, ölçülebilir performans metrikleri, neden analizi, sorun yönetimi ve iyi uygulamalar ve standartlarla karşılaştırmalardan oluşmaktadır (Iliescu, 2010: 95).

#### 4. LİTERATÜR TARAMASI

Bilgi teknolojileri yönetişimine ilişkin olarak ulusal ve uluslararası literatürde yer alan çalışmalara ilişkin özet bilgilere aşağıda yer verilmektedir. Yapılan araştırmada konu ile ilgili son derece sınırlı sayıda akademik çalışmanın mevcut olduğu ve bilgi teknolojilerinin denetimine yönelik kapsam önerisinde bulunan bir çalışmanın mevcut olmadığı görülmüştür. Bu açıdan değerlendirildiğinde, bu çalışmanın literatüre katkı sağlayacağı düşünülmektedir.

Kutsikos ve Bekiaris (2007) sanal organizasyonlarda bilgi teknolojileri yönetişiminin denetimine yönelik bir çalışma gerçekleştirmiştir. Çalışmalarının kapsamında bilgi teknolojileri yönetişim çerçevelerine yönelik açıklamalara yer verilmiş, organizasyonların yapılarındaki gelişmeler belirtilmiş ve bu gelişimin bilgi teknolojileri yönetişim süreçlerine olan etkisinin bir denetim çerçevesi yoluyla modellenmesi yapılmıştır.

Gheorghe (2010) organizasyonlardaki bilgi teknolojileri yönetişim süreçlerinin denetimine yönelik bir denetim yöntemi bulmuştur. Önerilen yöntem, bilgi teknolojileri yönetişim süreçlerinin etkinliğini ve yeterliliğini değerlendirmeye yönelik olarak hazırlanmış olup risk bazlı bir strateji içermektedir. Ayrıca, bu model ile süreçlerdeki risklerin değerlendirilmesi ve risklilik seviyesi artan bölümlerin tespit edilmesine olanak sağlanmaktadır.

Iliescu (2010) bilgi teknolojileri yönetişim süreçlerinin denetimine yönelik bir çalışma gerçekleştirmiştir. Çalışmada, işletmelerin bilgi teknolojileri yönetişim süreçlerinin denetçiler tarafından sağlıklı değerlendirilebilmesi için denetimi gerçekleştiren denetçilerin konuyla ilgili süreçlere, ilgili standartlara, denetim programlarını ve ortaya çıkan göstergeleri değerlendirme ve yorumlama yeteneğine sahip olmaları gerektiği sonucuna varılmıştır.

Heroux ve Fortin (2013) bilgi teknolojileri yönetişiminde iç denetim fonksiyonunun yeri ve önemine yönelik bir çalışma gerçekleştirmiştir. Anket yöntemi kullanılarak gerçekleştirilen araştırmada, iç denetim fonksiyonlarının bilgi teknolojileri yönetişim yapılarına, süreçlerine ve ilişkisel yeteneklerine katılımının yeterli düzeyde olmadığı sonucuna ulaşılmıştır. Bununla birlikte iç denetim biriminin kaynakları, personel tecrübesi, eğitim ve sertifikasyonları ve iç denetim ile kurum içerisindeki yönetim kurulu komiteleri arasındaki iletişimin, iç denetim fonksiyonunun bilgi teknolojileri yönetişimine katılımını etkileyen faktörler olduğu belirlenmiştir.

Kayrak (2013) bilişim teknolojileri yönetişimine ilişkin bir çalışma gerçekleştirmiştir. Çalışmada, bilgi teknolojileri yönetişiminin tanımına, bilgi teknolojileri yönetimi ile arasındaki farklılıklara, bilgi teknolojileri yönetişimine ilişkin kontrollere, standartlara ve bilgi teknolojileri yönetişimi alanlarına yer verilmiştir.

Amoroso, Bogale ve Kinfu (2015) Etiyopya'da bilgi teknolojileri ve bilgi teknolojileri yönetişim süreçlerinin denetimine yönelik bir araştırma gerçekleştirmiştir. Banka ve sigorta şirketlerinde yapılan anket uygulamaları sonucunda, bilgi teknolojileri yönetişim performansının denetim uygulamaları, üst yönetim kadrosunun nitelikleri, bilgi teknolojileri yönetişim uygulamaları ve çalışan sayısı ile ilişkili olduğu tespitine ulaşılmıştır. Çalışmada ayrıca bilgi teknolojileri denetimi, bilgi teknolojileri yönetişim çerçevesine dâhil edilmek suretiyle bir yönetişim çerçevesi geliştirilmiştir.

Jones (2015) bilgi teknolojileri denetiminin, bilgi teknolojileri yönetişim yapılarının iş planlarıyla paralel tasarlanmasına ve hedeflenen sonuçlara ulaşmasına yönelik güvence vermekten sorumlu olduğunu ifade etmektedir. Çalışma kapsamında, Uluslararası İç Denetçiler Enstitüsü'nün (IIA) kılavuzundan hareketle bilgi teknolojileri denetişim süreçlerinin denetlenmesine yönelik teorik uygulamalara yer verilmiştir.

Andry (2016) COBIT (Control Objectives for Information and Related Technology) çerçevesini baz almak suretiyle işletmelerde bilgi teknolojileri yönetim süreçlerinin denetimine yönelik örnek olarak seçilen bir eğitim merkezinde COBIT çerçevesinde bir vak'a çalışması gerçekleştirmiştir. Çalışma neticesinde, kurumun performans ve kapasitesinin yönetilememesi sonucu ortaya çıkabilecek olumsuz etkilerden haberdar olduğu, performans ihtiyaçlarının ilgili ekiplerin bilgisi ve bireysel sistemlerin değerlendirilmesi suretiyle karşılandığı sonucuna ulaşılmıştır.

Sholihat (2017) Endonezya'da bilgi teknolojileri yönetimi denetiminin uygulanmasına yönelik bir çalışma gerçekleştirmiştir. Çalışmada, Endonezya Maliye Bakanlığı'nın bilgi teknolojileri yönetim denetimine yönelik uygulamaları COBIT çerçevesi ile kıyaslanmış ve özellikle denetimlerin kapsamlarının belirlenmesi anlamında gelişim alanlarının mevcut olduğu sonucuna varılmıştır.

## 5. DENETİMLERDE BİLGİ TEKNOLOJİSİ YÖNETİŞİMİ KONUSUNDA VERİLECEK GÜVENCEYE İLİŞKİN BİR ÖNERİ

Bilgi teknolojilerinin gelişen ve karmaşıklaşan yapısı içerisinde bu alanda verilecek güvence hizmetlerinin de kapsamının gözden geçirilmesi gerekmektedir. Bugün bilgi teknolojileri denetim alanı pek çok alt alandan oluşmakla beraber bunlara çatı vazifesi gören ve bilgi teknolojileri faaliyetlerinin işletilmesinde kullanılacak yapıları belirleyen bilgi teknolojileri yönetimi diğer alt alanlarda tespit edilme potansiyeli barındıran problemlerin kök nedeni olması ve işleyişe ilişkin kurumsal kuralları ortaya koyması bakımından güvence sağlayıcılar açısından hem ayrı bir denetim alanı hem de diğer alanları değerlendirebilmek için incelenmesi gereken tamamlayıcı bir alandır.

Bu açıdan bakıldığında işletmelerde bilgi teknolojilerine yönelik organizasyonun gelişim seviyesine de bağlı olarak bilgi teknolojileri yönetimi denetimi ayrı bir denetlenebilir alan olarak değerlendirilebileceği gibi bilgi teknolojileri organizasyonu görece daha az olgunlaşmış işletmelerde diğer denetim alanlarının içerisinde bir alt alan olarak da dikkate alınabilir.

Bu çerçevede yürütülecek denetim çalışmalarında, ön hazırlık safhasından başlayarak çalışmanın planlanmasında hangi riskler yönünden incelemelerin gerçekleştirileceği ve ilgili denetim alanında hangi güvencelerin sunulacağı konusu hem kapsam belirlemede hem denetim kaynağının planlanmasında önemli bir konu haline gelmektedir.

Bilgi Teknolojilerinin şirket içerisindeki yönetsimsel yapısına ilişkin bir denetim çalışması aşağıdaki konuları içerebilecektir:

**Tablo 1: Bilgi Teknolojileri Yönetişim Alanında Denetimlerle Verilebilecek Güvenceler ve Bu Kapsamda Yürütülecek Çalışmalar**

Güvence Tanımı	Denetim Test Amacı Tanımı
<b>Sahiplik:</b> Yönetimin Bilgi Teknolojileri konularına sahipliği uygun seviyededir.	Yönetimde Bilgi Teknolojileri formasyonlu bir üye var mıdır? Yönetimin bilgi teknolojilerine ilişkin farkındalığı hangi seviyededir? Böyle bir sorgulama yönetim seviyesinde bilgi teknolojisi kaynaklı risklerin değerlendirilmesinde yeterli yetkinliğin bulunup bulunmadığını, bilgi teknolojilerinin işletme bünyesinde gelişmesi için yönetim seviyesinde gerekli desteğin verilip verilemeyeceğini sorgulamak için gündeme alınır. Bunu tespit etmek için yöneticilerle görüşmeler yapılır, şirkette bilgi teknolojilerinden sorumlu en üst düzey çalışanın bilgi teknolojilerine ilişkin stratejilerin belirlenmesinde ve uygulamaya alınmasında yaşadığı sorunları öğrenmek üzere görüşme gerçekleştirilir, yöneticilerin bilgi teknolojileri alanındaki yetkinliklerini belirlemek için özgeçmişleri incelenir, yönetim toplantılarında bilgi teknolojileri ile ilişkili konulara ne şekilde yaklaşıldığını anlamak üzere toplantı tutanakları incelenir. Bu yolla Bilgi Teknolojilerinin şirket içerisinde ne şekilde konumlandığı da ortaya koyularak bu yöndeki faaliyetlerin yönlendirilmesi ve takibi için uygun bir yapının kurulup kurulmadığı sorusu gündeme getirilir. Bu

Güvence Tanımı	Denetim Test Amacı Tanımı
	noktada yapılacak olası tespitler Bilgi Teknolojileri ile ilgili yapılacak pek çok tespit için bir kök neden oluşturabilir. Organizasyon şemasının incelenmesi ve Bilgi Teknolojileri yöneticisinin görev ve yetkileri ile raporlama hatlarının incelenmesi ile de bu sorgulamaya gidilebilir. Eğer şirkette bilgi teknolojileri üst yönetim seviyesinde bilgi teknolojileri uzmanlığı olan bir personele bağlı olarak yönetiliyorsa, bu çalışanın bilgi teknolojileri konusundaki görüşleri ve bilgi teknolojileri kaynaklı risklere yaklaşımları anlaşılmalı çalışılır.
<b>Stratejik Yönelim ve Uyumlanma:</b> Bilgi Teknolojileri ile ilgili her karar şirket ana stratejileri kapsamında performans sonuçlarını besleyecek yapısal bir şekilde verilmektedir.	İşletmede bir bilgi teknolojisi stratejisinin varlığı sorgulanır. Bilgi Teknolojileri Stratejisi, ana işletme stratejisini destekleyen bir alt stratejidir. Bu nedenle Bilgi Teknolojileri stratejisinin işletme stratejileri ile uyumlu olup olmadığı incelenir. İşletme stratejilerinde Bilgi Teknolojilerine atıfta bulunan konulara paralel şekilde Bilgi Teknolojileri stratejisinde de düzenlemeler olduğu test edilir. Bunun için; yazılı işletme stratejisinin ve Bilgi Teknolojileri stratejisinin varlığı, bilgi teknolojisi stratejilerinin onaylanma süreçleri, Bilgi Teknolojileri stratejisinin daha kısa vadeli taktik planlarla uyumu konuları göz önünde bulundurulur. Bilgi teknolojileri stratejisi ve buna dayanılarak hazırlanacak taktik planların bilgi teknolojileri alanında performans ölçümünü de belirleyecek şekilde alt kademelere doğru yayılması önemlidir. Ayrıca bilgi teknolojileri stratejisinden yola çıkılarak taktik planlarla beraber kaynak ihtiyaçlarının planlanması, süreçlerin belirlenmesi, bütçenin ortaya koyulması, dış kaynak alımının planlanması, performans ve kapasite yönetiminin planlanması, insan kaynakları yönetimi ve risk yönetimi gibi pek çok konunun ilişki içerisinde yürütülmesi beklenmektedir.
<b>Süreçler ve organizasyon:</b> Bilgi teknolojisi süreçleri ve organizasyonu bilgi teknolojileri stratejilerini destekleyecek şekilde yapısal bir şekilde oluşturulmuştur.	Stratejik yönelimler belirlendikten sonra beklenen iş çıktılarına ulaşabilmek için kullanılacak kaynaklar da göz önünde bulundurularak iş süreçleri oluşturulur. İş süreçleri amaçlara ulaşılması için yürütülen faaliyetler bütününe tanımlayan akışlar olup bunların organizasyonel yapılanma, görev tanımları, yetkiler, kontroller, iş hedefleri ve yetkinlikler gibi pek çok konu için belirleyici olduğunu göz önünde bulundurularak incelenmesi gerekmektedir. İncelemede iş süreçlerine ilişkin oluşturulan iş akış şemaları, prosedürler, talimatlar vb. doküman üzerinden yürütülebileceği gibi bilgi sistemlerine ilişkin dokümanite edilmemiş iş süreçlerinin ya da mevcut dokümantasyonda yer verildiği şekilde işletilmeyen süreçlerin belirlenmesi de önemlidir. İş süreç dokümanlarının uygun seviyelerde onaylandığı, uygun detay seviyesine sahip olduğu, dönemsel gözden geçirmelere tabi tutulduğu, işleyişe ilişkin prosedür ve talimatlara atıflar içerdiği, çalışanlar tarafından erişilebilir ve anlaşılabilir olduğu hususları değerlendirilir. Ayrıca iş akış dokümanlarının süreç içerisindeki ana kontrolleri içerip içermediği de incelenir.
<b>Rol ve Sorumluluklar:</b> Bilgi Teknolojilerine ilişkin sorumluluklar belirlenmiş, iş sahipliği sağlanmıştır.	Bilgi teknolojilerine ilişkin süreçler belirlendikten sonra bu süreçlerdeki roller bunlarla ilişkili şekilde tanımlanmış mıdır? Bunu anlayabilmek için işletmede kullanılan, RACI ve benzeri araçlar temin edilir ve incelenir. Tanımlanan yetkilerin belirtildiği şekilde kullanılıp kullanılmadığını anlamak üzere yetki alanlarına ilişkin işlemlerden örnekler seçilerek uygulamanın da bu kapsamda olduğu test edilir. Yetkilerin kullanımı sırasında potansiyel olarak çatışmaya sebep olabilecek alanlar tespit edilir. Bilgi Teknolojilerine ilişkin faaliyetler kapsamında sahipsiz kalan alanların olup olmadığı araştırılır.



Güvence Tanımı	Denetim Test Amacı Tanımı
<p><b>Bütçe:</b> İşletme kaynakları bilgi teknolojilerine yönelik ihtiyaçlar kapsamında ekonomik ve sistemli bir şekilde tahsis edilmekte ve kullanılmaktadır.</p>	<p>Bilgi teknolojileri taktik planın bir unsuru olan bilgi teknolojileri kaynak planlaması bilgi teknolojileri bütçesinin oluşturulmasında dikkate alınmış mıdır? Sürdürülecek, sonlandırılacak, yenilenecek, ilk defa tesis edilecek bilgi teknolojileri bileşenlerine ilişkin gerekli planlamalar yapılmakta mıdır? Bilgi teknolojileri bütçesinin oluşturulma aşaması yapısal bir şekilde kurgulanmış mıdır? Bilgi teknolojisi bütçesinin oluşturulmasına katılım gösteren paydaşlar uygun şekilde seçilmiş midir? Bilgi teknolojileri bütçesi uygun yönetim seviyelerince onaylanmakta mıdır? Bilgi teknolojileri bütçesi dâhilinde harcama/yatırım yapılması için gerekli satın alma karar sistemleri kurgulanmış mıdır? Bütçe kapsamında veya bütçe kapsamının dışında anlık olarak ortaya çıkabilecek ihtiyaçlar için yetki limitleri belirlenmiş midir? Bilgi teknolojileri bütçesinin izleme sorumlulukları tanımlanmış mıdır? Bilgi teknolojileri bütçesinin değişen ihtiyaçlar çerçevesinde revize edilmesine ilişkin kurallar belirlenmiş midir? Bu kapsamda yürütülecek test çalışmalarında bilgi teknolojileri bütçesi, bütçenin oluşturulma sürecine ilişkin detaylar, bütçenin kabulüne ilişkin onaylar, varsa bütçenin yıl içerisindeki revizyon talepleri, bütçenin takip sürecine ilişkin destekleyici dokümanlar, bütçede meydana gelen aşımaların ve bütçenin ilerleyişinin uygun yönetim kademelerine raporlandığına ilişkin kanıtlar, bütçe sürecine, yetki ve sorumluluklara ilişkin yazılı ve onaylı prosedürler aranır. Ayrıca taktik plan ve bütçe arasında bağlantılar kurulmaya çalışılır. Bütçe kapsamındaki harcamalardan örnekler incelenerek bütçe yönetim sisteminin işleyişteki başarısı üzerine değerlendirilmede bulunulur.</p> <p>Ayrıca, Bilgi Teknolojileri ile ilişkili kaynaklar projelere ne şekilde tahsis edilmektedir? İşletmede bir proje yönetim metodolojisi uygulanmakta mıdır? Projelerin tamamlanma başarısı ve iş modeli içerisinde tanımlanan faydayı gerçekleştirme başarısı ölçümlenmekte midir? Seçilen örnek projeler üzerinden proje yönetim karar süreçleri, projelerin kaynak kullanımlarının planlama başarıları, projelerin izleme ve revizyon süreçleri, projelerin tamamlanması sonrası beklenen-gerçekleşen fayda analizleri incelenip Bilgi Teknolojileri kaynak yönetimi ile proje yönetimi arasındaki ilişki anlaşılmaya çalışılır.</p>
<p><b>Performans izleme:</b> Bilgi teknolojilerinin performansının izlenmesine ilişkin kurgulanan araçlar yeterli ve çalışır durumdadır.</p>	<p>Şirket ana stratejileri ile uyumlu bir şekilde oluşturulan bilgi teknolojileri stratejileri ve buna bağlı taktik planlar çerçevesinde performans izleme sistemleri oluşturulur. Performans izleme sistemleri hem performans düşüklüklerini tespit etmede hem de işletmeye stratejik yönelim vermede etkili araçlardır. Bu kapsamda, dış kaynak yoluyla edinilenler de dâhil, bilgi teknolojileri hedeflerini izlemek için kullanılan performans göstergelerinin (KPI, SLA, OLA, v.b.) uygunluğu değerlendirilir. Performans hedeflerinin taktik planları desteklediği ve başarıyı taktik planların tarif ettiği şekilde formüle ettiği görülür. Ayrıca, performans ölçümüne ilişkin sorumluluklar incelenir. Performans düşüklüklerinde alınacak önlemlere ilişkin prosedürler ve performans yönetim sistematigi dikkate alınır.</p>
<p><b>Risk yönetimi:</b> Bilgi teknolojileri ile ilişkili risklerin izlenmesinde kullanılacak yapılar ihtiyaca uygun</p>	<p>Bilgi teknolojileri ile bağlantılı kayıp doğurabilecek potansiyel olaylar konusunda farkındalığın oluşması, risklerin tespit edilmesi, bunların olasılık ve etki yönünden değerlendirilmesi, bunlara uygun yanıtların verilmesi ve ihtiyaç halinde risklere portföy bakış açısıyla yaklaşılarak önceliklendirilmesi ve risklere karşı alınan önlemlerin kaynak maliyetlerinin yönetilmesi kapsamında yürütülecek çalışmalarda sorumlulukların tayini, uygun izleme ve değerlendirme mekanizmalarının kurulması, uygun raporlama hatlarının oluşturulması denetimlerde değerlendirilecek konulardır.</p>

Güvence Tanımı	Denetim Test Amacı Tanımı
şekilde kurgulanmış ve işletilmektedir.	Bu kapsamda yürütülen faaliyetlerin kapsamı ve süreç içerisindeki rol ve sorumluluklar incelenir.
<b>Yasal çevre:</b> Denetimler sonucu tespitler ve mevzuat değişiklikleri sonrası ihtiyaç duyulan geliştirmeler zamanlı bir şekilde yerine getirilmektedir.	Denetim sonrası oluşturulan aksiyon planlarının takibinden ve yasal otoritenin mevzuat değişikliklerinin takibinden sorumlular belirlenmiş midir? Gerekli aksiyonlar uygun şekilde dokümanite edilmekte ve süreç boyunca takip edilmekte midir? Zamanında tamamlanamayan aksiyonlar için uygun yönetim kademelerine raporlama yapılmakta mıdır? Bu durum aksiyon planlarını içeren dokümanlardan, mevzuat takibi ve uyum prosedürlerinden ve raporlama hatlarının ne şekilde işletildiğine ilişkin seçilen örnek olaylardan yola çıkılarak test edilir.

## 6. SONUÇ

Bilgi Teknolojilerinin günümüzde artan önemi bu konuda verilen güvence hizmetlerinin de çeşitlenmesine neden olmuştur. İşletmelerde bilgi teknolojilerinin yönetimi, organizasyonun bu alandaki olgunluk seviyesine bağlı olarak şekillenmektedir. Faaliyetlerini bilgi teknolojilerine bağımlı olarak yürüten işletmeler bilgi teknolojilerinin işleyişinde işletmenin amaçları yönünden istenilen çıktılara ulaşabilmek adına gerekli desteği sağlayacak yönde organize olarak yaşamlarına devam etmektedirler.

Bilgi teknolojilerinin yönetimi, bilgi teknolojileriyle ilişkili fonksiyonların işletme ile hizalı olarak faaliyet göstermesini ve işletme amaçlarına ulaşmada katma değer yaratmasını sağlamada, kaynakların etkili ve verimli şekilde kullanılmasında, görev ve sorumlulukların belirlenerek görev çatışmalarının ve sahipsiz kalan süreçlerin oluşmasını önlemede, hedeflerin işletme ihtiyaçları çerçevesinde belirlenmesinde, stratejik yönelimlerin bilgi teknolojileri fonksiyonu içerisinde yayılımında, performansın izlenmesinde, kaynak yönetiminde ve benzeri pek çok alanda gerekli yapıların kurulması ve gereğince işletilmesi için önem arz etmektedir.

İşletmeler açısından önem arz eden bilgi teknolojileri yönetimi, işletme ihtiyaçlarına göre ayrı bir denetlenebilir alan olarak ele alınabileceği gibi, diğer denetim alanlarının bir alt bileşeni olarak da değerlendirilebilir. Her durumda yapılacak çalışma ile sunulacak güvence hizmetinin kapsamının doğru şekilde belirlenmesi önem arz etmektedir. Bu sayede denetim çalışmasına tahsis edilecek kaynağın belirlenmesi de sağlanacaktır.

Çalışmanın amacı, bilgi teknolojileri yönetimi alanında verilecek güvence hizmetlerine yönelik olarak bir kapsam önerisinde bulunulması olarak belirlenmiştir. Bu amaçla, nitel araştırma yöntemlerinden doküman analizi yönteminden faydalanılmak suretiyle bu alanda yapılacak denetimlerde gerçekleştirilebilecek çalışmalara yönelik önerilerde bulunulmuştur. Bu çerçevede yürütülecek çalışmalarda önerilen bu kapsamdan yola çıkılarak denetimin amaçlarına da uygun bir şekilde planlama çalışmalarının yürütülmesi mümkün olacaktır.

**Hakem Değerlendirmesi:** Dış bağımsız.

**Çıkar Çatışması:** Yazarlar çıkar çatışması bildirmemiştir.

**Finansal Destek:** Yazarlar bu çalışma için finansal destek almadığını beyan etmiştir.

**Etik Onay:** Bu makale, insan veya hayvanlar ile ilgili etik onay gerektiren herhangi bir araştırma içermemektedir.

**Yazar Katkısı:** Kaan Ramazan Çakalı (%50), Gürol Baloğlu (%50)

**Peer-review:** Externally peer-reviewed.

**Conflict of Interest:** The authors declare that there is no conflict of interest.

**Funding:** The authors received no financial support for the research, authorship and/or publication of this article.

**Ethical Approval:** This article does not contain any studies with human participants or animals performed by the authors.

**Author Contributions:** Kaan Ramazan Çakalı (50%), Gürol Baloğlu (50%)

**KAYNAKÇA**

- Amoroso, D. L., Bogale, M. ve Kinfu, J. (2015). Auditing IT and IT governance in Ethiopia. Proceeding of the 12th IEEE 2015 AFRICON International Conference, 1–12.
- Andry, J. F. (2016). Audit of IT governance based on COBIT 5 assessments: a case study. *Beranda*, 2(2), 27-34. doi: 10.25077/TEKNOSI.v2i2.2016.27-34
- Aydın, N. (2018). Nitel araştırma yöntemleri: etnoloji. *Uluslararası Beşeri Ve Sosyal Bilimler İnceleme Dergisi*, 2(2), 60-71. Erişim Adresi: <https://dergipark.org.tr/tr/pub/ihssr/issue/36852/425401>.
- Celayir, D. (2021). *İç denetim ve risk değerlendirme*. Hiperlink.
- De Haes, S. ve Van Grennbergen, W. (2004). IT governance and its mechanisms. *Information Systems Control Journal*, 1, 1-7. Erişim Adresi: <https://blog.dinamika.ac.id/erwin/files/2013/02/jpdf041-ITGovernanceandIts.pdf>.
- Gheorghe, M. (2010). Audit methodology for IT governance. *Informatica Economica, Academy Of Economic Studies*, 14(1), 32-42. Erişim Adresi: [https://www.researchgate.net/publication/43121541\\_Audit\\_Methodology\\_for\\_IT\\_Governance](https://www.researchgate.net/publication/43121541_Audit_Methodology_for_IT_Governance).
- Heroux, S. ve Fortin, A. (2013). The internal audit function in information technology governance: a holistic perspective. *Journal Of Information Systems*, 27(1), 189–217. doi: 10.2308/isisys-50331
- Hunton J. E., Bryant S. M. ve Bagranoff N. A. (2004). *Core concepts of information technology auditing*. John Wiley & Sons Inc.
- IIA. (2018). *Global technology audit guide*. The Institute of Internal Auditors Global. Erişim Adresi: <https://www.iaa.nl/SiteFiles/GTAG%2017%20Auditing%20IT%20Governance.pdf>.
- IIA. (2019). *Uluslararası mesleki uygulama çerçevesi*. Türkiye İç Denetim Enstitüsü Derneği.
- Iliescu, F. M. (2010). Auditing IT governance. *Informatica Economica*, 14(1), 93-102. Erişim Adresi: [https://www.researchgate.net/publication/43121547\\_Auditing\\_IT\\_Governance](https://www.researchgate.net/publication/43121547_Auditing_IT_Governance).
- ITGI (2003). *Board briefing on IT governance*. Erişim Adresi: [https://eventosfehosp.com.br/2017/material/sao\\_paulo/ti/jose/ITGI-Instrucoes-de-Governanca-de-TI-para-a-Alta-Administracao.pdf](https://eventosfehosp.com.br/2017/material/sao_paulo/ti/jose/ITGI-Instrucoes-de-Governanca-de-TI-para-a-Alta-Administracao.pdf).
- ITGI (2007). *IT governance using COBIT and val IT*. Student Book.
- Jones, R. (2015). Auditing IT governance structures. *Orbus software white paper*, WP0217, 1-6. Erişim Adresi: [https://cdn-ow-prod-ooj2.azureedge.net/assets/docs/default-source/blogs/wp0217-auditing-it-governance-structures-.pdf?sfvrsn=d20b2873\\_0](https://cdn-ow-prod-ooj2.azureedge.net/assets/docs/default-source/blogs/wp0217-auditing-it-governance-structures-.pdf?sfvrsn=d20b2873_0).
- Kayrak, M. (2013). Bilişim teknolojileri yönetişimi. *Sayıştay Dergisi*, (91), 57-76. Erişim Adresi: <https://dergipark.org.tr/tr/pub/sayistay/issue/61546/919138>.
- Kutsikos, K. ve Bekiaris, M. (2007). IT governance auditing in virtual organizations. *Management Of International Business And Economic Systems Transactions*, 1(1), 35-45. Erişim Adresi: [https://www.researchgate.net/publication/242068986\\_IT\\_Governance\\_Auditing\\_in\\_Virtual\\_Organizations](https://www.researchgate.net/publication/242068986_IT_Governance_Auditing_in_Virtual_Organizations).
- NCC (2005). *IT governance: developing a successful governance strategy*, NCC.
- Özbek, Ç. (2012). *İç denetim kurumsal yönetim risk yönetimi iç kontrol*. Türkiye İç Denetim Enstitüsü Yayınları.
- Sholihat, N. I. (2017). The implementation of information technology governance audit in the ministry of finance of Indonesia. *Simposium Nasional Akuntansi*, 20, 1-20. doi: 10.33312/ijar.341

## **SUMMARY**

### **Introduction**

In this study, a special sub-area of the Information Technologies, IT governance, is considered. Assurance services on Information Technologies governance auditable area need to be customized and auditors who provide this assurance need to be specialized. This study presents a recommendation on definitions of assurance on which auditors will focus during IT governance audits.

### **Literature Review**

In academic literature, number of studies on auditing IT governance is very limited. Kutsikos and Bekiaris (2007) analyzed the relationship between the IT governance frameworks and organizational structures. Gheorghe (2010) proposed a methodology in evaluating IT governance processes. Iliescu (2010) concluded that auditors need special skills in evaluating IT governance processes. Heroux and Fortin (2013) studied on importance of the internal auditors within IT governance structure. Amoroso, Bogale and Kinfu (2015) performed a survey study and concluded that audit performance depends on the variables like qualifications of top-management, IT governance structure and number of staff. Jones (2015) reported a theoretical background for IT governance audits depending on the Institute of Internal Auditors' guidelines. Andry (2016) performed a case study and showed that performance needs match with knowledge of teams and personal systems. Sholihat (2017) compared COBIT framework and Indonesian Finance Ministry's IT governance practices.

### **Internal Audit and IT Audit**

Auditing information technologies is one of the main parts of internal audit. IT audits cover all technological infrastructures, security, software, hardware, and similar components. IT audits evaluate general IT controls and application controls.

### **IT Governance**

IT Governance helps IT structures meet with organizational objectives and integrate information Technologies with business processes. It may be defined as a sub-process of the corporate governance. IT Governance is closely related with monitoring IT related risks and managing IT resources also. Five core areas are defined for IT governance:

- Strategic alignment: Combining IT strategies and business objectives.
- Value creation: Delivering value under the predetermined budget conditions.
- Risk management: Managing potential adverse effects.
- Resource management: Managing IT resources in an effective and efficient way.
- Performance management: Measuring and managing the value of the IT in an organization.

### **A Recommendation: Assurance on IT Governance Provided by the Audits**

IT Governance can be considered as an individual auditable object or a sub-area of the other IT related auditable objects. In each circumstance, assurance level that the auditor wants to serve needs to be pre-determined in a preparation phase of the audit. A recommendation on assurance level is presented below:

**Table 1: Assurances Provided and the Audit Works Performed During the Audits of IT Governance**

<b>Definition of Assurance</b>	<b>Audit Objective to Assure that:</b>
Ownership	Senior Management's ownership for IT related issues is at a desired level. Awareness of senior management in IT related issues allows risk management procedures to be conducted effectively. Support from senior management allows IT environment to be improved. Positioning of the IT in the organization allows IT to be represented effectively.
Strategic alignment	IT related decisions support business objectives. IT Strategy is aligned with the business strategy. Approval process for the IT Strategy is defined. IT Strategy is cascaded to tactical plans to ensure IT Strategies span over the organization. Tactical plans are tied with performance management systems, IT budgets, outsourcing decisions, capacity management, resource management, human resource management in IT, risk management, etc.
Processes and organization	IT processes and organization support IT strategies. Considering strategic and tactical preferences and available resources, the company is organized the required structures and defined its workflows. Workflows are related with other documents, like job definitions, authorities, targets, procedures, policies, control matrixes etc. Annual review of all corporate documents is performed. All documents are accessible by the related stakeholders.
Roles and responsibilities	Roles and responsibilities in IT related issues are defined. Conflict of interest potentials are eliminated. All issues are attached to at least one responsible.
Budget	IT resources are allocated and used in an efficient and effective way. Resource planning is an integral part of the IT tactical planning. Budgeting processes are organized in a structural way. Monitoring of the budget is performing. IT Budget and project management are aligned.
Performance management	Systems and tools for IT performance management are satisfactory. Performance indicators are determined aligning with tactical plans to ensure required strategic direction is given. Targets are well-defined in formulizing the success. Action plans against low performance are defined.
Risk management	Frameworks used for IT risk monitoring is defined as needed. Potential adverse effects of the incidents are realized, measured as probability and effect. Responses and reporting lines are also defined.
Regulatory compliance	Actions against audit findings and changes in regulations are planning in a timely and efficient way. Reporting lines are defined for irregularities.

### Conclusion

Depending on the increasing importance of the IT, assurance services on this area become more sophisticated. IT Governance is an integral part of the IT and the problems experienced in this area generally affect other IT related areas. Thus, IT governance is started to be considered as a unique auditable object, besides being a sub-area of other IT related areas. Serving assurance on IT governance needs a proper planning for determining both level of assurance and resource planning in audits. In this study, a recommendation for assurance level on IT governance is presented. Practitioners need to be customized the assurance level depending on the maturity level of the audited company.