KAMUDA DİJİTAL DÖNÜŞÜMÜN SİBER GÜVENLİK VE DİJİTAL GÜVENCE BOYUTLARI VE İÇ DENETİMİN ROLÜ

(THE DIGITAL TRANSFORMATION IN PUBLIC SECTOR WITH THE DIMENSIONS OF CYBER SECURITY AND DIGITAL TRUST AND THE ROLE OF INTERNAL AUDIT)

Serhat AKMEŞE*

ÖZ

Günümüzde kamu sektörü önemli bir dijital dönüşüm süreci içerisindedir. Bu yolculuk beraberinde vatandaş odaklı hizmet modeli ve veri analitiği uygulamalarını gündeme getirmektedir. Söz konusu durum, kurumların faaliyetlerine ilişkin risk radarlarında dijital güvence ve siber güvenlik gibi alanların öne çıkmasına sebep olmaktadır. Gelecekte, iç denetim fonksiyonunun kurumlarına sağlayacağı katma değeri, siber güvenlik ve dijital güvence risklerine ilişkin verilen güvence ve danışmanlık faaliyetlerinin etkinliği ile değerlendirmek gerekecektir. Bu çalışmada, kamu sektörünün içerisinde olduğu dijital dönüşüm yolculuğunun temel bileşenleri tartışılmakta ve iç denetimin siber güvenlik ve dijital güvence alanında organizasyona nasıl katkı sağlayabileceği değerlendirilmektedir.

Anahtar Kelimeler: Dijital Dönüşüm, Siber Güvenlik, Dijital Güvence, Vatandaş Odaklı Kamu Hizmet Yönetimi, İç Denetim.

JEL Kodları: O32, O38

ABSTRACT

Government and public sector is in a journey of digital transformation. This journey will bring citizen based service model and data analytic applications into agenda. This situation let government institutions prioritize digital trust and cyber security risks in their operations. In the future, the added value of internal audit will be directly related with the efficiency of assurance and advisory services delivered to the institutions by internal audit entities in the areas of cyber security and digital trust. This study, assess the main dimensions of digital transformation and evaluates the main services that internal audit deliver in cyber security and digital trust.

Keywords: *Digital Transformation, Cyber Security, Digital Trust, Citizen Based Public Services Management, Internal Audit.*

JEL Classification: *O32, O38*

* CIA, CISA, CGAP, CRMA, CICA, PMP, SMMM, EY Danışmanlık Hizmetleri Yardımcı Ortak, Ankara, Orcid Id: 0000-0001-6884-8380, serhat.akmese@tr.ey.com Yazı Gönderim Tarihi: 15.04.2019, Yazı Kabul Tarihi: 17.04.2019

1. GİRİŞ

Dünyada yaşanan teknolojik gelişmeler vatandaşın kamu hizmet sunumuna yönelik beklentilerini hızla değiştirmektedir. Bu değişimi gerektiren temel unsurlar iki ana konu başlığı altında değerlendirilebilir.

Bunlardan biri, **internete erişim ve mobil uygulamalara olan talepteki artış**tır. Tüm dünyada internet kullanıcılarının sayısı yıllık ortalama % 4,8 artarak 4 milyar kullanıcıyı aşmıştır (Broadband Commission, The State of Broadband, 2015). Benzer şekilde dünyada akıllı telefon kullanımı da her yıl ortalama %15 artmaktadır. Mobil telefon kullanıcılarının sayısı ise 2018 itibari ile 5 milyarı aşmıştır (Global Digital Report, 2018).

Kamu hizmetlerinde dijital dönüşümü tetikleyen diğer unsur ise, **bilgi teknolojilerine yönelik maliyetlerdeki tasarruf baskısı**dır. Tüm dünyada devletler, gelirlerin yönetimi, vatandaşa yönelik hizmetler, satın alma gibi alanlarda dijital çözümler ile maliyetlerini azaltmaya çalışmaktadırlar. Bir başka ifadeyle, tüm dünyada devletler etkin hizmet sunumu, maliyet azaltımı ve kamu hizmetlerinin kaliteli şekilde verilebilmesi için dijital dönüşüm çalışmalarını mevcut politika gündemlerinde üst sıralara almışlardır.

Kamu hizmetlerinin dijital platformlar üzerinden sunulmasını ifade eden dijital dönüşüm sürecinde, teknoloji ve bilgi güvenliği risklerini kurumların risk radarlarında ön sıralara getirmektedir. Bu çerçevede, kurumların risk yönetimi süreçlerinin dijital, teknoloji ve siber güvenlik boyutları çalışmanın bir diğer tartışma konusudur. İç denetim birimlerinin de güvence ve danışmanlık faaliyetlerini bu çerçevede planlamaları, iç denetimin kamu yönetimindeki rolünü güçlendirmesi bakımından önem arz etmektedir. İç denetim faaliyetlerinin, kurumların içinde olduğu bu dijital dönüşüm sürecinde, katma değer sağlayabileceği alanlar da teknoloji riskleri ve siber güvenlik boyutları ile değerlendirilmiştir.

Kamu kurumlarının dijital dönüşümünde, iç denetim faaliyetinin rolünü değerlendiren bu çalışmanın ilk kısmında, kamu hizmet sunumunda dijital dönüşümün temel yapı taşları ve başarı göstergeleri, güncel uygulamalar ve ülke deneyimleri çerçevesinde değerlendirilmektedir. Kamu hizmet sunumunda, vatandaş deneyimi yaklaşımının kurumların dijital dönüşümündeki stratejik hedeflerden biri olması dolayısıyla çalışmanın ikinci kısmında, vatandaş deneyimi odaklı hizmet sunumunun maliyet ve verimlilik açısıyla avantajları değerlendirilmektedir.

2. KAMU HİZMET SUNUMUNDA DİJİTAL DÖNÜŞÜM

Kamu hizmet sunumunda, dijital dönüşüm eğilimlerini en yoğun yaşadığımız alanlar aşağıdaki gibi sıralanabilir.

Kamu mali yönetimi: Gelir idaresine yönelik hizmet sunumunda kullanılan bilgi teknolojileri altyapısının etkinleştirilmesi, büyük veriye dayanan risk yönetim sistemlerinin tasarlanması ile kayıt dışı ve suiistimalin azaltılması amacıyla gerçekleştirilen dijital dönüşüm uygulamaları bu çerçevede değerlendirilebilir.

Dünya Bankası tarafından yapılan, küresel ölçekte 198 devleti kapsayan bir araştırmada, kullandıkları kamu mali yönetim sistemleri aracılığı ile bütçelerini şeffaf şekilde paylaşabilen ve iyi uygulama olarak değerlendirilebilecek ülkelerin oranı %12 olarak tespit edilmiştir[2](Dener, Min Saw Yoang, 2013, s. 17).

Altyapı ve ulaşım: Özellikle akıllı şehirler ve ulaşım planlamaları hali hazırda devletlerin gündemindeki öncelikli dijital dönüşüm alanlarından biridir.

Savunma ve siber güvenlik: Gelişen teknolojiler ile artan siber güvenlik riskleri günümüzde devletlerin risk radarında siber güvenliği en üst sıralara yerleştirmiştir.

Eğitim: Eğitim hizmetlerine erişimin artırılması ve e-öğrenme uygulamaları, bilgi teknolojileri altyapılarında dönüşüm gerektiren hizmet alanları arasında yer almaktadır.

2.1. Kamuda Dijital Dönüşümün Başarısını Belirleyen Temel Unsurlar

Kamu sektöründe, dijital dönüşümün başarısını belirleyici unsurlardan biri, dijital dönüşümü kendi içlerinde entegre olmayan uygulama ve projeler yerine, iş yönetiminin bir parçası olarak kabul etmektir. Bu bakış ile tasarlanan bir dijital dönüşüm sürecinde kurumların odaklandıkları beş temel alan aşağıdaki gibi özetlenebilir:

1. **Strateji;** kamu yönetimi ve hizmet sunumunda, kurumsal hedefler ve iş yönetimi stratejisi dijital yaklaşım ile uyumlu şekilde tasarlanmaktadır.
2. **İnovasyon;** kurumların değişen vatandaş beklentisi ve teknoloji gereksinimlerine cevap verecek yenilikçi çözümler üretebilen hizmet sunumu modellerinin geliştirilmesi olarak değerlendirilebilir. Akıllı şehir projeleri bu kapsamdaki dijital dönüşüm süreçleri için en iyi örnekler arasında yer almaktadır.
3. **Vatandaş deneyimi**; kamu hizmet sunumunda, vatandaşların değişen beklentilerini en hızlı şekilde hizmet sunumuna entegre edecek veri analizi ve yönetimi kapasitesinin geliştirilmesidir.
4. **Hizmet sunumu;** dijital teknolojiler, mevcut kamu hizmet sunumunda maliyet ve verimlilik avantajı sağlanacak şekilde süreç ve operasyonlara entegre edilmektedir.
5. **Güvence;** kurumların içinde oldukları dijital dönüşüm serüveninde, yönetmek durumunda oldukları risklerin değerlendirilmesi, gerekli aksiyonların planlanması ve izlenmesi ise, baştan sona dijital dönüşüm sürecinin başarılı olabilmesi için en önemli unsurlardan biridir.

Ülkelerin yaşadıkları dijital dönüşüm sürecine ilişkin birçok örnek üzerinden iyi uygulama deneyimleri paylaşılabilir. Örneğin; Hindistan'da EY (Ernst & Young) tarafından gerçekleştirilen çalışmada, Kamu mali yönetimi kapsamında, kamu kurumlarına yönelik 300 adet anahtar performans göstergesinin sadece kurum yönetimi ve iş süreci sahipleri tarafından değil aynı zamanda vatandaş tarafından da eş zamanlı olarak izlenmesi ve raporlanması mümkün hale gelmiştir. Benzer şekilde, e-devlet iyi uygulamalarında öne çıkan Estonya'da gerçekleştirilen vatandaş bütçesi yaklaşımı da vatandaşların kamu harcamalarını şeffaf şekilde izlemesine imkân vermektedir.

2018 yılında IIA (Uluslararası İç Denetçiler Enstitüsü) tarafından gerçekleştirilen, 311 iç denetim yöneticisini anket ve 42 iç denetim yöneticisinin de görüşme ile katkı sağladığı, "Risk in Focus 2019" araştırmasında da sadece kamu değil özel sektörde de dijital dönüşümün getirdiği belirsizliklerin kurumların risk radarlarında öncelikli alanlardan biri haline geldiği görülmektedir.

Bu araştırmada iç denetçilerin %66'sı kurumlarında en önemli 5 risk arasına siber güvenlik ve %58 ile veri güvenliğini almışlardır. Dijitalleşme de %36 ile öne çıkan risk alanları arasında ifade edilmiştir (IAA, 2018, s. 3).

Benzer şekilde, EY tarafından, Dünya Bankası finansmanında, İç Denetim Koordinasyon Kurulu liderliğinde gerçekleştirilen iç denetim araştırmasında kamu iç denetçilerinin %22'si bilgi teknolojilerinin, kurumların risk evrenleri içerisinde öncelikli olarak yer alacağını belirtmişlerdir. Burada iç denetçilerin %15'i siber güvenlik alanını kurumların öncelikli riskleri arasına almışlardır. İç denetçiler, gelecek 5 yıl içerisinde kurumlarına en fazla değer katacak denetim türleri arasında %54 ile BT denetimini göstermişlerdir (İDKK, 2018).

Araştırmada öne çıkan genel tespit, robot süreç otomasyonu, yapay zeka, makine öğrenmesi gibi çözümlerin, organizasyonda yeni belirsizlikler meydana getirdiğidir. Özellikle, bu seviyede karmaşık uygulamalara geçen organizasyonlar, risk yönetimlerinde bu alanlara hakim iç denetçilerin güvence ve danışmanlık faaliyetlerine daha fazla ihtiyaç duymaktadırlar.

2.2. Kamuda Dijital Dönüşüm Sürecinde İç Denetim

İç denetim fonksiyonu, organizasyonun yaşadığı dijital dönüşümde, strateji katmanından güvence aşamasına kadar etkin bir güvence sağlayıcı ve danışman olarak yer alabilir. İç denetçinin buradaki rolü, kurumun dijitalleşme sürecinde yer aldığı aşamaya göre değişiklik arz edebilir. Bu dönüşümde iç denetim tarafından sorulması gereken temel sorular aşağıdaki gibi sıralanabilir:

- Bu dönüşüm içerisinde, kamu idarelerinin kullanacakları yeni teknolojiler, organizasyonun stratejisi ile uyumlu mudur?
- Yeni teknolojilerin getirdiği belirsizlikler ve riskler doğru değerlendirilmiş midir?
- Vatandaş odaklı yenilikçi çözümler doğrultusunda, kurumların iç kontrol sistemlerinin yeniden gözden geçirilmesi gerekmekte midir?

- Kamu hizmet sunumunda kullanılan yeni teknolojilerin, sağladığı maliyet ve verimlilik avantajlarına yönelik performansları doğru şekilde değerlendirilebilmekte midir?
- Dijitalleşme süreci ile değişen siber güvenlik ve teknoloji riskleri etkin şekilde yönetilebilmekte midir?

Kurumların içinde olduğu dijital dönüşüm sürecinde, iç denetim fonksiyonlarının en yoğun şekilde yer aldığı alan, dijital riskler ve siber güvenlik riskleridir. Kurumların bu dönemlerde yaşadıkları temel zorluklar:

- Bu alanda, uyumsuzlukların yönetilmesi ve itibar kaybına sebep olabilecek kontrol zayıflıklarının tespit edilememesi,
- Veri yönetimi sürecinin ve veri kaynaklarının güvenliğinin ve kontrol ortamının iyileştirilememesi,
- Siber saldırılara dayanıklı yapıların oluşturulamaması,
- Yaşanan dijital dönüşümde kurumların değişen risklerini zamanında, doğru şekilde tespit edememeleridir.

3. VATANDAŞ DENEYİMİ ODAKLI KAMU HİZMET SUNUMU ÇERÇEVESİ

Vatandaş deneyimi, bireysel ya da kurumsal şekilde, vatandaşın iş ya da özel hayatında, devlet ile temas ettiği tüm alanları kapsamaktadır. Devletin doğrudan veya dolaylı olarak kontrolü ve sorumluluğu olan tüm temas ve iletişim bu çerçevede yer almaktadır.

Vatandaş deneyimi, vatandaşların istek ve taleplerine göre kamu hizmetlerinin ve kamu politikalarının tasarlanmasını amaçlar. Bu bakımdan, vatandaş deneyiminin temel hedefleri, kamu hizmet yönetiminde kalitenin artırılması, vatandaş ile şeffaf ve verimli bir etkileşim sağlanması ve vatandaşın kamu hizmet sunumuna olan güvenini ve memnuniyetini artırmaktır.

Vatandaş deneyimi 3 ana konu başlığı altında incelenmektedir.

1. **Hizmet sunumu**; Bu alanda kamu hizmet sunumu kapsamında değerlendirebilecek, devletin doğrudan kontrolü altında olan, nüfus, vatandaşlık gibi hizmetler yer alabilir.
2. **Hizmet ekosistemi;** Devlet tarafından bireylere ve organizasyonlara sunulan ulaşım, sağlık, güvenlik gibi temel hizmetlerdir.
3. **Yasa ve mevzuatsal çerçeve;** Kamu politikalarına yönelik uygulamalar, düzenleyici mevzuat ve yasalardır.

İngiltere Hükümeti tarafından yayınlanan dijital verimlilik raporunda, vatandaş ile kurulacak temasın dijital kanallar ile gerçekleşmesinin, bir telefon görüşmesinden 20 kat, posta ile iletişimden 30 kat ve yüz yüze görüşmeden 50 kat daha az maliyetli olduğu belirtilmiştir[3] (Digital Efficiency Report, 2012).

Aynı şekilde, hizmet verimliliğinin de diğer yöntemlere kıyasa dijital süreçler ile %50 daha verimli olduğu ifade edilmektedir. Bu nedenle, İngiltere Hükümeti, 2020 itibari ile tüm kamu kurumlarının yarısından fazlasında ve özellikle doğrudan vatandaş ile etkileşimi olan kurumlarda, kurum bütçelerinin %25'ini teknoloji platformları ve yenilikçi teknolojilere ayırmayı hedeflemektedir.

Vatandaş deneyimi bakışı ile tasarlanan bir dijital dönüşüm süreci vatandaş ve kamu gözü ile değerlendirildiğinde öne çıkan avantajlar aşağıdaki gibi sıralanabilir.

Vatandaşlar açısından;

- Kamu hizmetine farklı kanallardan ulaşabilme,
- Yalın şekilde tasarlanmış iş süreçleri,
- Hızlı hizmet sunumu ve sorun çözümü

hususları öne çıkmaktadır.

Kamu hizmet sunumu açısından bakıldığında ise;

- Vatandaşlara daha kaliteli hizmet sağlayabilmek,
- Hizmet sunumu memnuniyeti ve kurum itibarını artırmak,
- Çalışan verimliliği,
- Çalışan memnuniyeti,
- Maliyet avantajı

hususları ön planda olmaktadır.

Dijital dönüşüm sürecinde kamu kurumlarının iş süreçlerine ve operasyonlarına dâhil edecekleri ya da faaliyetlerini destekleyecek uygulamalar ve bu uygulamaların sağlayabileceği katma değer aşağıdaki gibi özetlenebilir:

- **Büyük veri ve analitik;** Verinin kişiselleştirilebildiği platformların geliştirilebilmesi için kullanılabilmesi,
- **Robot süreç otomasyonu;** Tekrar eden ve manuel olarak yürütülen aktivitelerin, işlemlerin azaltılması,
- **Yapay zekâ;** Vatandaşlara, daha proaktif, hızlı ve kişiselleştirilmiş geri dönüşlerin sağlanabilmesi,
- **Bulut teknolojisi**; Vatandaş erişiminin sağlanabileceği açık veri portallarının tasarlanabilmesi,
- **Nesnelerin interneti;** Vatandaş deneyiminin daha iyi anlaşılabilmesi için veri üretilmesi ve hizmetler geliştirilmesi,
- **Makine öğrenmesi;** Vatandaşa yönelik hizmetlerdeki eğilimlerin ve tercihlerin daha doğru ve hızlı analiz edilebilmesi,
- **Chatbot;** Kamu hizmetinde sanal hizmet sunucuların işlemleri gerçekleştirebilmesi.

4. DİJİTAL GÜVENCE KAVRAMI/ FAALİYETLERİ

Dünyadaki birçok devlet gibi ülkemiz de, tüm kamu kurumlarımız ile birlikte bir dijital dönüşüm yolculuğundadır. Fakat yeni dönemdeki dijital uygulamalar bazı mevcut risklerin etkilerini ve gerçekleşme ihtimallerini artırmakla birlikte, kurumların radarlarına yeni riskler de getirmişlerdir. Kurumlardaki geleneksel risk yönetimi mekanizmaları çoğunlukla gelişen bu risklerin izlenmesi ve gerekli aksiyonların alınması konusunda yeterli katkıyı gösterememektedir.

Bu süreçteki temel zorluklar aşağıda belirtilen hususların yeteri kadar anlaşılamaması ve değer görmemesinden kaynaklanmaktadır.

- Dijital dönüşümün kamu kurumlarımız için günümüzde bir seçim değil zorunluluk olması,
- Dijital teknolojiler ve bu teknolojilerin getirdiği riskler,
- Risk fonksiyonlarının da artık dijital yaklaşım ve çözümlere ihtiyaç duymaları.

Dolayısıyla, organizasyonların bu zorluklara karşı, doğru kurgulanmış bir dijital risk yönetimi yaklaşımı ve çerçevesi geliştirmeleri gerekmektedir.

4.1. Dijital Güvence Faaliyeti

İç denetçiler olarak paydaşlara sağlanacak dijital güvence faaliyetleri ile kurumların yönettikleri dijital programları için önemli bir güvence ve danışmanlık hizmeti sağlanabilecektir. Böylece, kurumların dijital dönüşüm yolculuklarında, yönetimin dijital programların tasarımı, uygulanması ve sürdürülebilirliğine yönelik nitelikli bir güvence ve danışmanlık hizmeti almasına imkân sağlanacaktır.

Dijital güvence faaliyetleri temel olarak iki soru üzerinden yapılandırılabilir:

- Operasyon modeli, kurumların amaç ve hedefleri, stratejik planları, insan kaynakları yaklaşımları ve kapasiteleri, dijital dönüşüm stratejileri ile uyumlu mudur?
- Veri, organizasyon, veriye ulaşım ve kullanım, zamanında, tam ve doğru veri yönetimi, veri güvenliği ve izlenebilirliği açısından doğru yaklaşım ve teknik kapasiteye sahip midir?

Günümüzde gerçekleştirilen dijital risk yönetimi yaklaşımları, risk analitiğine verdikleri önem ile fark yaratmaktadırlar. Bu yaklaşım, reaktif olarak tasarlanmış risk yönetimi bakışının yerine, dijital teknolojileri ve veri analitiğini içeren proaktif risk yönetimi olarak özetlenebilir. Kullanılan yeni teknolojiler ve yöntemler risk yönetimi sisteminin daha dinamik olmasına imkân vermektedir.

4.2. Dijital Risk Yönetimi Faaliyeti

Dijital risk yönetimi faaliyetinin temel aşamaları aşağıdaki gibi özetlenebilir:

- Risk değerlendirme kriterlerinin belirlenmesi,
- Değerlendirme kapsamındaki bilgi teknolojileri süreçlerinin belirlenmesi,

  - o Yönetişim,
  - o Bilgi teknolojileri iş süreçleri,
  - o Gizlilik,
  - o Uyum,

- Değerlendirme yöntem ve araçlarının belirlenmesi, değerlendirmeye katılacak tarafların ve grupların tespit edilmesi,
- Değerlendirmeye katılacak taraflara farklı araç ve teknolojiler ile ulaşılarak değerlendirmeye esas görüş ve tespitlerin alınması,
- Gelen değerlendirme ve tespitlerin konsolide edilmesi,
- Belirlenen alanlara göre risk derecelendirmelerin gerçekleştirilmesi,
- Yapılan analizlere yönelik değerlendirmeler ve çalıştayların gerçekleştirilmesi,
- Veri analizleri ve çalıştaylardan edinilen geri bildirimler ile risk derecelendirmelerinin gerçekleştirilmesi,
- Risk derecelendirilmelerinin validasyonları,
- Risk raporlarının ve ısı haritalarının oluşturulması.

Dijital dönüşüm yolculuğunda karşılaşılabilecek risklere karşı dayanıklı ve etkin olduğunu düşünen bir organizasyon için doğru sorular şu şekilde sıralanmaktadır:

a- Dijital dönüşüm sürecinde, organizasyonun dijital dönüşümün getirdiği riskleri en iyi şekilde yönetebilmesine imkân verecek, operasyon modeli ve stratejisi tasarlanmış mıdır?

Organizasyonun dijital dönüşüm ve veri odaklı bir yaklaşım takip edebilmesi için, dijital dönüşüm stratejisinin organizasyonun mevcut operasyon ve faaliyetlerinin tamamını kapsayacak şekilde planlanması önem arz etmektedir. Bu amaç ile tasarlanmış bir organizasyon stratejisinin aşağıdaki gerekliliklere ve kısıtlara cevap verebilmesi gerekmektedir.

- Organizasyonun, amaç ve hedeflerine ulaşabilmek için yeterli perspektifi sağlayacak bir dijital risk yönetimi anlayışı var mıdır?
- Dijital risk yönetimi stratejisi, mevcut karar alma süreçlerine girdi sağlayabilecek şekilde dinamik olarak tasarlanmış mıdır?
- Organizasyon, mevcut kurumsal öncelikleri ile uyumlu şekilde risklerini izleyebilmekte midir?
- Kurumun geleceğine yönelik sürdürülebilir başarısı için ne tür bir kaynak yönetimi ve kontrol kültürü tesis edilmelidir?
- Dijital risk yönetimi yaklaşımı gelecekte, organizasyonun 3 seviyeli güvence (üçlü savunma hattı) yaklaşımına nasıl entegre edilmelidir?

b- Vatandaş ve hizmet alıcıya sağlanacak güvence için nasıl bir yapı ve kontrol ortamı tasarlanmıştır?

Kurumlarda vatandaş odaklı dönüşüm süreci, vatandaşın veri güvenliği ve hizmet sürekliliği anlamında asgari beklentilerinin karşılanmasına yönelik güvence verilmesi ile başlamaktadır. Bu çerçevede tasarlanan bir yapıda;

- Vatandaşın ve hizmet alıcıların alışkanlıkları ve beklentilerinin doğru şekilde tespit edilmesi,
- Bu öncelik ve eğilimlere göre hizmet stratejisinin tasarlanması,
- Belirlenen hizmet stratejisine uygun operasyon modelinin tasarlanması,
- Bu operasyon modelinin üzerinde koşacağı teknoloji altyapısının ve mimarinin planlanması,

vatandaş odaklı dönüşüm ve dijital risk yönetimi bakımından öncelikli girdiler/sorular arasında değerlendirilebilir.

Bu çerçevede kurgulanacak bir yapıda, vatandaşa şeffaflık, veri ve hizmet kalitesi açısından güvence sunabilecek bir iş modeli tasarlamak için cevap verilmesi gereken kısıtlar ve öncelikler şunlardır:

- Dijital dönüşüm süreci, organizasyona ne tür avantajlar sağlayacaktır?
- Organizasyon içinde olduğu dijital dönüşüm süreci için nasıl bir dijital güvence mekanizması tasarlamıştır?
- Vatandaş ve tüm paydaşlar açısından şeffaflık ve etkin güvenceyi esas alan bir yapı için ne tür

stratejik öncelikler bulunmaktadır ve bu önceliklerin belirlenmesi ve yönetiminde kimin ne tür sorumlulukları vardır?

- Mevcut risk yönetimi ve kontrol mekanizması dijital süreçlere ne seviyede aktarılmıştır ve dijital iş süreçleri ile ne seviyede entegre olmuştur?
- Risk ve uyum açısından değerlendirildiğinde, dijital hizmetlerin mevcut mevzuat ve kanunlara uyumu nasıl değerlendirilmektedir?

c- Hizmet verimliliği ve etkin kontrol ortamının sağlanabilmesi için ne tür teknoloji ve veri analitiği yatırımları yapılmaktadır?

Risk yönetimi mekanizmalarının temel amaçlarından biri, organizasyonun karşılaştığı fırsat ve tehditlerin yönetimi için alınacak aksiyonlarda, karar vericileri zamanında ve doğru şekilde bilgilendirmektir. Böylece değişen koşullarda yönetimin fırsat ve tehditleri başarılı şekilde yönetebilmeleri sağlanabilir.

Risk yönetimi mekanizması ile dinamik ve gerçek zamanlı şekilde beslenen bir karar destek yapısı için eden kısıtlar ve unsurlar aşağıda belirtilmiştir:

- Mevcut risk yönetimi yaklaşımı, vatandaş, temel paydaşlar ve düzenleyici mevzuata uyum açısından etkin bir güvence sağlayabilmekte midir?
- Risk yönetimi yaklaşımı, yönetimin değişen koşullarda doğru karar verebilmelerini sağlayacak, nitelikli ve etkin raporlama bilgilendirme kabiliyetine sahip midir?
- Mevcut risk verisi, organizasyondaki üçlü savunma hattında yeterli şekilde analiz edilebilmekte midir?
- Dijital risk yönetimi yaklaşımı, mevcut riskleri gerçek zamanlı olarak izleyebilmekte ve ileriye dönük analiz ve tahminler yapabilmekte midir?

Yukarıda belirtilen, gerçek zamanlı ve veri analitiğine dayanan risk yönetimi sistemi için kullanılan veri ve teknoloji ekosistemi önem arz etmektedir. Ancak dijital ekosistem ile entegre bir sistem, analizler için doğru veriye sahip olabilir ve böylece hem hizmet performansı hem de etkin güvence sağlanabilir. Mevcut teknoloji ekosistemi içerisinde, kullanılan kurumsal kaynak planlama sistemi, algoritmalar, süreç otomasyonu teknolojileri, bulut mimarisi ve dış veri platformları yer almaktadır.

Kullanılan veri ve teknoloji mimarisinin aşağıdaki sorulara doğru cevap vermeleri gerekmektedir.

- Organizasyonun günlük faaliyetlerinde, stratejik hedefleri ile uyumlu iş süreçlerine daha fazla odaklanmasını sağlayacak ne tür teknolojiler yer almaktadır?
- Kullanılan veri ve teknoloji güvenilir midir?
- Mevcut veri ve teknoloji, organizasyonda devam eden dijital dönüşüme ne tür stratejik katkılar sağlayabilir?
- Dijital dönüşüm sürecindeki uyum risklerini etkin yönetebilmek için mevcut risk verisi nasıl kullanılabilir?
- Yeni nesil teknolojiler, organizasyonun risklerini daha etkin yönetebilmelerine katkı sağlayabilir mi?
- Geliştirilen teknoloji platformu, organizasyondaki üçlü savunma hattına doğru şekilde entegre olabilir mi ve değer yaratabilir mi?

d- Organizasyon, gelebilecek tüm saldırı ve tehditlere sürdürülebilir ve sürekli şekilde cevap verebilmekte midir?

Siber güvenlik ve iş sürekliliği alanları, dijital dönüşüm sürecinde öncelikli riskler arasında yer almaktadır.

Bu alanlardaki riskleri ve risklerin etki ve olasılıklarını etkileyen hususlar aşağıdaki gibi sıralanabilir:

- Kurumların taşra teşkilatlarının varlığı, hizmet seviyeleri gibi lokasyon karakteristikleri,
- İnsan kaynaklarına ilişkin izleme ve teknoloji yetkinlikleri,
- İş süreçlerinde yönetilen verinin önem seviyesi ve siber saldırılara maruz kalma oranları,
- Üçüncü taraf hizmet yükümlülükleri.

Bu çerçevede tasarlanacak bir dijital risk yönetimi için temel bileşenler ve strateji unsurları aşağıdaki gibi değerlendirilebilir:

- Günümüzün kamu hizmet sunumu döngüsünde riskler nasıl ölçülmektedir?
- Organizasyon, tüm hizmet sunumu ve operasyon bileşenleri ile risklere karşı dayanıklı hale getirilebilir mi?
- Hizmet sunumunun sürekliliği açısından mevcut risk portföyü nasıl değerlendirilmektedir.
- Gelecekte organizasyonun dönüşümü ile birlikte, iş sürekliliği stratejisi de bu dönüşüme uygun şekilde değişim gösterebilir mi?

5. KAMUDA DİJİTAL DÖNÜŞÜMÜN SİBER GÜVENLİK BOYUTU

Kamu sektöründe, kurumların öncelikli riskleri arasında yer alan temel alanlardan biri hiç şüphesiz siber güvenliktir. 2021 yılında, siber suçların küresel ekonomiye zararının 6 Trilyon $ olacağı öngörülmektedir. Siber saldırılara en fazla maruz kalan 5 sektör şunlardır[4](Cybersecurity Ventures Official Annual Cybercrime Report, 2018):

- Sağlık
- Üretim
- Finansal Hizmetler
- Kamu
- Ulaşım

Siber güvenlik riskleri açısından, kamu sektörünün önündeki yapısal sorunlar arasında aşağıdaki hususlar öne çıkmaktadır:

- Siber güvenliğe ilişkin yeterli farkındalık oluşmamıştır ve güçlü mevzuatsal düzenlemelere ihtiyaç vardır.
- Siber saldırılara dayanıklı kurumsal ve teknolojik yapıların kurulabilmesi için yeni yatırımlara ihtiyaç vardır.
- Yeterli insan kaynağına ulaşımda zorluklar yaşanmaktadır.

Bununla birlikte sürekli yöntem değiştiren ve karmaşıklaşan siber saldırılara karşı daha dinamik bir yapının kurulması zorunluluk haline gelmektedir. Yapılan saldırıların karmaşıklığının artması, nesnelerin interneti ve dijital teknolojiler ile siber saldırılara maruz kalabilecek verinin boyutunun artması gibi hususlar, kamu sektöründe yaşanan siber saldırıların boyutunu değiştirmekte ve etkisini artırmaktadır.

Kamu kurumları, siber saldırılara ve tehditlere cevap verebilmek için sürekli geliştirmelere yatırım yapmaktadır. Fakat bu tarz saldırılara karşı duyarlılığı artırmak, dayanıklılığı güçlendirmek ve saldırılara en hızlı şekilde reaksiyon verebilmek için sürekli odaklanmaya ve iyileştirmelere ihtiyaç vardır. Kamu kurumlarının siber güvenlik alanında ajandalarında yer alan öncelikli konuları ise aşağıdaki gibi sıralanabilir:

- Siber dönüşüm
  - Kurumların faaliyet gösterdikleri alan ve hedeflerine göre siber güvenlik stratejilerinin ve yol haritalarının geliştirilmesi,
  - Siber güvenlik programlarının etkinliğinin ve verimliliğinin değerlendirilmesi,
  - Kurumun iş süreçlerini ve siber güvenlik faaliyetlerini düzenleyen üçüncül düzey mevzuatlar ve yönetmelikler,
  - Siber güvenlik farkındalığı ve eğitimleri.
- Siber saldırı yönetimi
  - Kurumlarda ortak hizmet merkezi şeklinde faaliyet gösteren güvenlik operasyonları merkezleri,
  - Nesnelerin interneti uygulamaları,
  - Güvenlik faaliyetlerinin izlenmesi,
  - Güvenlik açıklarının tespiti ve yönetimine yönelik mekanizmaların tesis edilmesi,
  - Yazılım güvenliği.
- Kimlik ve erişim yönetimi
  - Strateji ve yönetişim,
  - Yetki ve rollerin etkin şekilde izlenebilmesine imkân verecek mekanizmaların oluşturulması,
  - Kimlik ve erişim yönetimi mimarisi ve uygulamaları,
  - Raporlama ve analizler.
- Verilerin korunması ve gizlilik
  - Veri kaybını önlemeye yönelik değerlendirmeler,
  - Veri güvenliği programlarının değerlendirilmesi ve geliştirilmesi,
  - Veri güvenliği teknolojilerinin uygulanması.

- Reaksiyon
  - o İş sürekliliği yönetimi kapasitesinin ve iş sürekliliği yönetimi çerçevesinin geliştirilmesi,
  - o Siber saldırılara karşılık verilebilmesine yönelik süreçlerin geliştirilmesi.

6. SİBER GÜVENLİK RİSKLERİNİN YÖNETİMİNDE İÇ DENETİMİN ROLÜ

Kurumların içinde oldukları dijital dönüşüm sürecinde, üst yönetimin radarında yer alan öncelikli risklerden birinin siber güvenlik olduğu görülmektedir. Siber güvenlik risklerine yönelik, iç denetim olarak etkin bir güvence ve danışmanlık hizmeti sunabilmek ve iç denetçiler olarak katma değeri artırabilmek için iç denetçilerin bu alandaki teknik bilgi ve deneyimlerinin sürekli geliştirilmesi gerekmektedir.

Günümüzde, siber güvenlik risklerinin etkisi ve boyutları sürekli değişmektedir. Zira siber güvenlik saldırıları bireysel faaliyetlerin ötesine geçmekte ve organize eylemler halini almaktadır. Saldırıların ağırlığı sadece finansal kayıplara yol açmamakta, itibar ve kurumların sürekliliği anlamında etkiler de oluşturmaktadır. Gelişen yeni nesil teknolojiler, siber güvenlik anlamında yeni çözümler getirmekle birlikte yeni riskleri de beraberinde getirmektedir.

Yaşanan büyük siber kayıplara bakıldığında, saldırıların erken tespit edilmesine karşın, zafiyetlerin ve boşlukların zamanında kapatılamamasından kaynaklı, kurumların daha etkili siber saldırılara açık hale geldiği ya da kurumların siber saldırılara daha dayanıklı olabilmek için önemli teknoloji yatırımları yapmalarına karşın bu teknolojileri etkin şekilde kullanamadıkları vakalar öne çıkmaktadır. Burada **iç denetim fonksiyonun odaklanması gereken temel alanlar** aşağıdaki gibi sıralanabilir.

6.1. Yönetişim

Organizasyonların siber güvenlik açısından dirençli hale gelebilmeleri için öncelikli hususlardan biri üst yönetim seviyesinde siber güvenlik konusunda farkındalık oluşturulmasıdır. Burada her bir iş biriminin, kurumun siber güvenlik risklerine dayanıklı olabilmeleri için almaları gereken aksiyonlar bulunmaktadır. İç denetim tarafından üst yönetim seviyesinde değerlendirilmesi gereken siber güvenliğe ilişkin hususlar aşağıdaki gibi özetlenebilir.

- Üst yönetici için, kurumun amaç ve hedefleri ile stratejik planlarının siber güvenlik açısından değerlendirilmesi,
- Kurumun mevcut hizmet sunumu ve operasyon modelinin içerisine siber güvenlik katmanının entegre edilmesi,
- Siber güvenlik açısından kurumun mevcut mevzuat ve prosedürlerinin gözden geçirilmesi,
- Olası siber güvenlik zararları ve kayıplara karşı yeterli sigorta ve güvence planlamalarının gerçekleştirilmesi,
- Mevcut teknolojinin gelişen siber güvenlik saldırılarına karşı ne kadar etkin olduğunun sürekli olarak izlenmesi ve değerlendirilmesi,
- Dijital dönüşüm sürecinin getirdiği risklerin siber güvenlik gözüyle değerlendirilmesi,
- Siber güvenliğin, üçlü savunma mekanizması ile nasıl entegre edileceğinin değerlendirilmesi,
- İç denetimin siber güvenliğe yönelik odaklanmasının planlanması,
- Siber güvenlik ile ilgili teknoloji yatırımının yanında insan kaynağı yatırımının da gerçekleştirilmesi,
- Siber güvenliğe yönelik organizasyon seviyesinde farkındalığın oluşturulması.

Üst yönetimin yukarıdaki sorulara doğru cevaplar verebilmesi ve etkin şekilde aksiyon alabilmesi için ilk etapta yapması gerekenler ise;

- Siber güveliğe ilişkin risk toleransının belirlenmesi ve onaylaması,
- Siber risklerin ölçülmesi ve değerlendirilmesi,
- Siber risklere yönelik daha şeffaf ve dinamik bir raporlama yapısının tesis edilmesi,
- Üst yönetim seviyesinde, siber güvenliğe ilişin yetkilendirme ve görevlendirmelerin gerçekleştirilmesi,
- Kurum seviyesinde siber güvenliğe yönelik farkındalığın artırılmasına destek verilmesi

olarak belirtilebilir.

6.2. Temel Kontrol Aktiviteleri

Siber saldırılara dayanıklı kurumlarda uygulanan ve iç denetimin değerlendireceği temel kontrol aktiviteleri aşağıdaki gibidir:

- Bilgi teknolojileri genel kontrolleri ile mevcut sistemlerin verinin gizlilik, tamlık ve doğruluk açısından mevcut mevzuat ve prosedürler ile uyumlu olup olmadığının değerlendirilmesi,
- Erişim ve yetkilerin yönetimi ile yönetici yetkileri dâhil olmak üzere tüm yetkilerin izlenebilmesi, erişime ilişkin şifre ve diğer gerekliliklerin güncel ihtiyaçlara göre sürekli gözden geçirilmesi,
- İzleme ile mevcut sistemlerin, yetkisiz erişim ve diğer boyutları ile sürekli olarak izlenebilmesi,
- Dijital varlık yönetimi mekanizmalarının geliştirilmesi,
- Kişisel verilerin korunması kapsamında gerekli yasal ve uygulama bazlı kontrollerin ve işlemlerin gerçekleştirilmesi.

6.3. Üçüncü Taraf Risk Yönetimi

Kurumların hizmet aldıkları üçüncü taraf hizmet sağlayıcılarının, siber güvenlik riskleri açısından sahip oldukları zafiyetler çoğunlukla kurumlar için de önemli risk alanları arasında yer almaktadır. Zira bu tarz üçüncü taraf hizmet sağlayıcılar ile veri paylaşımı ve sistemsel entegrasyonlar gerekmektedir. Bu nedenle, organizasyonda, alt yüklenici, hizmet sağlayıcı, dış kaynak kullanımı ya da sözleşmeli olarak çalışan tüm tarafların bu çerçevede kurumun siber güvenlik süreçleri ile uyumlu bir kontrol ortamına sahip olmaları gerekmektedir.

Bu açıdan değerlendirildiğinde, üst yönetim ve iç denetim için öncelikli sorular aşağıdaki gibi sıralanabilir:

- Organizasyon, hizmet sunumu veya mevcut operasyonları içerisinde yer alan tüm üçüncü taraf hizmet sunucularına ilişkin bir envantere sahip midir?
- Üçüncü taraf hizmet sağlayıcılar ile paylaşılmış ve siber güvenlik risklerine karşı alınacak aksiyon ve beklentileri içeren açık ve net bir prosedür bulunmakta mıdır?
- Üst yönetim ve organizasyon üçüncü taraf hizmet sağlayıcılarından kaynaklı olarak oluşabilecek risklerin farkında mıdır? Bu riskler etkin şekilde ölçülmekte ve izlenmekte midir?

6.4. Sürdürülebilirlik

Siber güvenlik risklerine yönelik günlük faaliyetlerden organizasyonel önceliklere kadar birçok alanda, faaliyetlerin sürdürülebilirliği kritik önem arz etmektedir. Sürdürülebilirlik, kurumların değişen şartlar ve saldırılara karşı çok hızlı tepkiler vererek hedeflenen hizmet sunumu seviyesini korumak veya en hızlı şekilde bu seviyeye gelebilmek olarak ifade edilebilir.

Faaliyetlerin sürdürülebilirliği için yönetim ve iç denetim tarafından göz önünde bulundurulması gereken öncelikli hususlar şu şekilde özetlenebilir:

- Siber güvenlik gözüyle sürdürülebilirliği etkileyebilecek alanların yönetimi ve zafiyetlerin ortadan kaldırılmasına yönelik sürekli iyileştirme çalışmaları,
- Sürdürülebilirlik risklerinin etkin şekilde izlenmesi ve değerlendirilmesi,
- Sistemlere yönelik sürdürülebilirlik risklerinin tespit edilmesi ve bilgi teknolojileri mimarisinin bu açıdan incelenmesi,
- Üçüncü taraf ve diğer bağımlılıkların siber güvenlik gözüyle değerlendirilmesi,
- Saldırıların tespit edilmesi ve sürekli raporlanması,
- Sistemlerin geri dönüş planlamalarının sürekli olarak test edilmesi.

6.5. Siber Risk Yönetimine Yönelik Bakış Açısının Günümüz İhtiyaçlarına Göre Gözden Geçirilmesi

Sürekli gelişen ve karmaşıklaşan siber güvenlik risklerine karşı kurumlarda yeni bir bakış açısının geliştirilmesi gerekmektedir. Yeni bakış açısının temel bileşenleri aşağıdaki gibi özetlenebilir:

- Siber güvenlik risklerinin ve bu risklere ilişkin kontrol faaliyetlerinin statik olarak ve organizasyonun operasyonundan ayrı bir yapı ile izlendiği ve uygulandığı bir yaklaşımdan ziyade siber güvenlik risklerini organizasyonun yöne-

tişimi içerisinde değerlendirmek ve siber güvenlik risklerinin organizasyonun operasyon modeline ve hizmet sunumuna etkilerini bir bütün olarak ele almak gerekmektedir.

- Siber güvenlikte odağın mevzuata uyumun ötesinde, yönetişim ve uygulamaya kaydırılması gerekmektedir.
- Siber güvenliğe ilişkin risklerin birbirinden kopuk ve çoğu zaman mükerrer kontroller gerçekleştiren yapılar yerine, ortak hizmet merkezi olarak çalışan siber güvenlik operasyonları merkezi tarzında yapılar ile yönetilmesi gerekmektedir.
- Mevcut durumda kurumların maruz kaldıkları siber saldırılara ilişin aksiyonlar alınırken, küresel eğilimler ve değişen saldırı yöntemleri sürekli izlenerek gelecekte kurumların siber saldırılara dayanıklı olmalarını sağlayacak aksiyonlar da ihmal edilmemelidir.

7. SONUÇ

Ülkemizde, kamu kurum ve kuruluşları, önemli bir dijital dönüşüm süreci içerisindedirler. İnternete erişim ve mobil uygulamalara olan talepteki artış ile birlikte vatandaşların kamu hizmet sunumuna yönelik beklentileri de değişmektedir. Kamu kurumlarımız gerek değişen vatandaş beklentilerine cevap verebilmek ve gerekse artan hizmet sunum maliyetlerini optimize edebilmek için dijital dönüşüm çalışmalarına öncelik vermektedirler.

Kamu mali yönetimi, altyapı ve ulaşım, siber güvenlik, eğitim gibi temel hizmet sunumu alanları bu süreçten en yoğun şekilde etkilenmişlerdir. Kurumların yaşadığı bu değişim ve dönüşüm süreci, kurumların dijital güvence ve siber güvenlik alanlarına yönelik riskleri daha etkin şekilde izlemelerini gerekli kılmaktadır.

İç denetim fonksiyonunun, gelişen siber güvenlik risklerine yönelik yürüteceği güvence ve danışmanlık faaliyetleri, kurumların söz konusu riskleri etkin şekilde izleyebilmesi ve gerekli aksiyonları alabilmesi için önem arz etmektedir. İç denetimin siber güvenlik süreçlerine yönelik denetim ve danışmanlık faaliyetlerinde, günümüzde siber güvenlik kayıplarının ana nedenlerini ve genel eğilimleri dikkate alarak denetim plan ve programları geliştirmeleri gerekmektedir.

Kurumların siber güvenlik risklerine yönelik belirleyici unsurlar ve dolayısıyla iç denetim tarafından dikkate alınması gereken hususlar aşağıdaki gibi özetlenebilir:

- Karmaşıklaşan teknoloji uygulamaları ile siber saldırıların yöntemleri de gelişmektedir.
- Dağınık bilgi teknolojileri mimarisi ve üçüncü taraf hizmet sağlayıcılar ile siber saldırılara maruz kalınan alanlar genişlemektedir. Ayrıca bu durum, siber güvenliğe ilişkin kontrol faaliyetlerinin baştan uca tüm sistemler ile entegre edilememesine sebep olmaktadır.
- Veri mevcudiyeti ve kalitesinde yaşanan yetersizlikler, siber güvenlik saldırıların tespit edilmesi ve önlenmesindeki zafiyetleri beraberinde getirmektedir.
- İnsan kaynağı yetersizlikleri, organizasyonların başarılı bir siber güvenlik stratejisi uygulamalarını zorlaştırmaktadır.

Sonuç olarak, günümüzde siber saldırıların etkileri; dijitalleşen iş süreçleri, süreç otomasyonu, veri güvenliği ve gizliliği gibi unsurlar sebebiyle değişmektedir. Yukarıda belirtilen unsurlar çerçevesinde iç denetim fonksiyonun, kurumun siber güvenlik stratejisine yönelik güvence ve danışmanlık hizmetini yeterli düzeyde sağlayabilmesi durumunda, etkin bir teknoloji ve dijital risk yönetimi mekanizmasının geliştirilmesine yardımcı olmak suretiyle kuruma ve üst yönetime sağlayacağı katma değer artabilecektir.

Kaynakça

Dener C., Min Saw Yoang, (2013). *Financial Management Information Systems and Open Budget Data*. Wahington, D.C., Dünya Bankası.

Broadband Commission, The State of Broadband (2015). Switzerland,

https://www.broadbandcommission.org/Documents/reports/bb-annualreport2015.pdf adresinden alındı. (Erişim tarihi, 15.04.2019).

İDKK, (2018). Kamu İç Denetim Reform Uygulamalarının Derinleştirilmesi Projesi, Kapsamlı değerlendirme raporu, Ankara, EY.

http://www.idkk.gov.tr/SiteDokumanlari/Manset/DB-

Konferans2018/ProjeSonucRaporu.pdf, adresinden alındı. (Erişim tarihi, 15.04.2019).

IIA, (2018). Risk in Focus 2019, UK, EIAA.

https://www.iia.org.uk/media/1689824/risk-in-focus-2019.pdf, adresinden alındı. (Erişim tarihi, 15.04.2019).

Global Digital Report (2018). We Are Social, https://digital-report.wearesocial.com/ adresinden alındı. (Erişim tarihi, 13.04.2019).

Cybersecurity Ventures Official Annual Cybercrime Report, (2017).

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, adresinden alındı. (Erişim tarihi, 12.04.2019).

Digital Efficiency Report, (2012). UK, Cabinet Office,

https://ofti.org/wp-content/uploads/2012/12/13281_digital-efficiency-report.pdf, adresinden alındı. (Erişim tarihi, 10.04.2019).

Cybersecurity Ventures Official Annual Cybercrime Report, (2017).

https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/, adresinden alındı. (Erişim tarihi, 12.04.2019).