DERLEME MAKALE

YÖNETİŞİM, RİSK VE UYUM KAPSAMINDA İÇ DENETİMİN DİJİTAL DÖNÜŞÜMÜ

DIGITAL TRANSFORMATION OF INTERNAL AUDIT WITHIN GOVERNANCE, RISK AND COMPLIANCE

Çiğdem İLHAN*

ÖZ

Sürekli gelişen teknolojik değişimlerle birlikte iş dünyasında da dijital dönüşümlerin hız kazanması, küresel ekonomi ve artan rekabet unsurları gibi belirsizlik ortamının oluşumu, şirketler için yeni risk faktörlerini de gündeme getirmektedir. Bir sorunun çözümlenmesine o sorunun kaynağına inmekle başlarız. Ancak iş dünyasındaki sorunlar karmaşık ve kapsamlı olabildiği gibi çözümleri de aynı ölçüde kapsamlılık gerektirebilmektedir. Sorunların farklı çözüm perspektifleriyle değerlendirilmesi ise ancak işletmelerin bütünleşik ve entegre sistemler vizyonuyla mümkündür.

İşletmelerin hedeflerine ulaşmasını destekleyen karmaşık sorunlara çözümler aramak için farklı organizasyonel sistemlerin birbirleriyle ilişkilendirilmesine izin veren Yönetişim Risk ve Uyum (Göverenince, Risk and Compliance – GRC)'ye dayalı metodoloji uygulanması gereklidir. Bu çalışma, dijitalleşen dünyada, şirketlerin dijital dönüşümlere ve yeni teknolojik çözümlere ayak uydurmasının öneminin yeterince anlaşılmaması, teknolojik çözümleri tüm süreçlerine yeterince uygulayamaması ve çağın gereklerinin dışında kalması gibi sorunları içermektedir. Çalışmanın amacı, işletme faaliyetlerinin, kurumun hedeflerine ulaşmasından, ihtiyaçlarını karşılama noktasına kadar, tüm süreçlerde entegre GRC model ve teknolojik çözümlerin kurum ve iç denetçiler bakımından değerlendirilmesidir. Makalede geleneksel yönetim ve denetim anlayışından, teknolojik çözümlerle, bütünsel bir yönetim anlayışına geçilmesinin, güçlü karar sistemlerinin geliştirilmesindeki katkısı

* SMMM, Ankara Sosyal Bilimler Üniversitesi, Sosyal Bilimler Entitüsü, Denetim ve Risk Yönetimi Anabilim Dalı, cigdemilhan1@gmail.com, ORCID: https://orcid.org/0000-0002-4346-760X.

Makale Geliş Tarihi : 08.11.2022
Kabul Tarihi : 09.03.2023

ve önemi ortaya koyulduğu gibi, güncel teknolojik çözümleri temeline alan risk yönetimi sistemlerine duyulan ihtiyacı da ortaya koymaktadır. Bu yaklaşım belirsizlik ortamında, kurumlardaki iç denetim mekanizmalarının etkinliğine sunduğu katkısı ile kuruma değer katma misyonu bakımından iç denetçiler açısından nitel bir araştırma çerçevesinde literatür analizi tekniği ile bütüncül bir bakış açısını esas alarak değerlendirme yapılmıştır.

Anahtar Sözcükler: GRC, Yönetişim, Risk, Uyum, İç Denetim, Dijital Dönüşüm

ABSTRACT

Along with the constantly developing technological changes, the acceleration of digital transformations in the business world, the formation of an environment of uncertainty such as the global economy, and increasing competition bring new risk factors to the agenda for companies. We begin to analyze a problem by going to the source of that problem. However, problems in the business world can be complex and comprehensive, and their solutions may require the same degree of comprehensiveness. Evaluating the problems from different solution perspectives are only possible with a holistic view and integrated systems vision of the enterprises.

It is necessary to apply Governance, Risk and Compliance (GRC) based methodology that allows different organizational systems to be interrelated to seek solutions to complex problems that support businesses in achieving their goals. This study includes problems such as the lack of understanding of the importance of companies keeping up with digital transformations and new technological solutions in the digitalizing world, not being able to apply technological solutions to all their processes adequately, and staying out of the necessities of the age. The aim of the study is to evaluate the integrated GRC model and technological solutions in all processes from the point of view of the institution and internal auditors, from the achievement of the enterprise's objectives to meeting its needs. In the article, the contribution and importance of the transition from the traditional management and audit approach to a holistic management approach with technological solutions are discussed for the development of strong decision systems, as well as the need for risk management systems based on current technological solutions. This approach has been evaluated within the framework of qualitative research for

internal auditors in terms of its contribution to the effectiveness of internal audit mechanisms in institutions and its mission to add value to the institution in an environment of uncertainty.

Keywords: GRC, Governance, Risk, Compliance, Internal Audit, Digital Transformation

1. GİRİŞ

Küreselleşmeyle birlikte iç ve dış ticarette artan rekabet ortamı, teknolojik gelişmeler, yasal düzenlemeler ve uygulamalarla, dijitalleşen yeni dünya düzeni, yeni normallerimizin de sınırlarını çizmiştir. Dijital çağın yaşandığı yeni dünya dinamikleri aynı zamanda kurumlardaki yönetim ve denetim anlayışını da değişime zorlamaktadır. Değişken, Belirsiz, Karmaşık ve Muğlak (Volatility, Uncertainty, Complexity, Ambiguity – V.U.C.A) bir dönemden geçtiğimiz günümüz şartlarında, şirketlerin değişime hızlı ve doğru karar mekanizmalarıyla adapte edilmesinin önemi ortaya çıkmaktadır. Zira bu dönem fırsatlarla birlikte riskleri de barındırmaktadır. Değişimin ve rekabetin iç içe yaşandığı bu belirsizlik ortamında, değişime aynı hızla uyum sağlanması oldukça önemlidir. Uyum sağlanamaması halinde mevcut durumunda risk altına gireceği unutulmamalıdır. Ancak risklerini ve fırsatlarını doğru yönetebilen kurumlar, bu dönemden çıkabilmekte olup, daha da güçlenebilme şansı yakalarlar.

Bu doğrultudaki yönetim ve denetim anlayışında, değişimlere paralel, entegre çözümler optimize edilerek, risklerin yönetiminde çağın gereklerine uyum sağlanmalıdır. Risk odaklı denetim anlayışının, GRC gibi gelişen teknolojik çözümlerle daha proaktif bir denetim anlayışına dönüştürülmesi ihtiyacı açıktır.

Makalenin birinci bölümünde, kavramsal çerçeve ve Açık Uyum ve Etik Grubu (Open Compliance and Ethics Group – OCEG) teorisine yer verilmiştir. İkinci bölümde, GRC Yapılanma Süreci; Dijitalleşme, GRC Yazılımları ile birlikte GRC öncesi ve sonrasına yönelik işletme yapılanması ile iç denetim yapılanmasından bahsedilmiştir.

2. KAVRAMSAL ÇERÇEVE VE OCEG TEORİSİ

2.1 Yönetişim

Uluslararası İç Denetçiler Enstitüsü (International Institute of Internal Auditors – IIA) 'nün iç denetim tanımında yönetişime vurgu yapılmaktadır. İç denetimi, bir işletmenin faaliyetlerine değer katma ve geliştirme amacını güden, objektif ve bağımsız bir güvence ve danışmanlık faaliyeti olarak, işletmenin kontrol, risk yönetimi ve yönetişim süreçlerinin etkinliğini değerlendirerek, geliştirmek amacıyla sistemli ve disiplinli bir yaklaşımla işletme amaçlarına ulaşmasına yardımcı olur şeklinde tanımlamaktadır (IIA, 2022, s.1).

Yönetişim, kökünde İngilizce olmayan, Türkçe kelimelerden türetilmiş yönetim ve iletişimden gelmektedir. Yönetim kelimesinden ''yönet'' iletişim kelimesinin ''işim'' eklerinden Türkçe kelime olarak türetilmiştir. Kapsamlı tanımlamak gerekirse yönetişim; örgütsel amaçların, kişilerin kişisel çıkarlarının üzerinde tutulduğu, etkileşimin olduğu, güven ve şeffaflığın benimsendiği, ortak akıl ile karar verilen, empat, proaktif ve sinerjik yaklaşımların gerçekleştiği örgütsel faaliyetlerdir olarak tanımlanabilir (Fidan 2011, s.6).

Riske dayalı, objektif güvence, tavsiye veya iç görü sağlayarak organizasyonel değeri artırmak ve korumak misyonuyla hareket eden iç denetçilerin, iç denetim tanımında belirtildiği üzere, iç kontrol, risk yönetimi, yönetişim süreçlerinin etkinliğinin değerlendirilmesi ve artırılması, iç denetçilerin sorumluluğunda görülmektedir. Yine aynı tanımda iç denetçilerin, temsil ettiği kurumları organizasyonel yapılarında başarıya ulaştıracak, güncel değişimlerin hızına ayak uyduracak her türlü teknolojik çözümlere odaklanması ve organizasyona kazandırması, kuruma değer katma misyonunun icrası bakımından kendilerine stratejik avantajlar sağlayacaktır. GRC süreçlerinin oluşturulması ve etkinliğinin sağlanması noktasında iç denetçiler kritik noktada yer almaktadırlar (Gökdeniz, Kartal ve Yetiş 2017, s.66).

Yönetişim aynı zamanda yatırımları, finansal istikrar ve iş etiğini geliştirerek şeffaflık ve hesap verilebilirliğin oluşturulmasına destek olan, bu sayede büyümeyi destekleyen bir yönetim çerçevesidir (OECD, 2015a, s.7; Aktaran, Gökdeniz, Kartal ve Yetiş 2017, s.65). Aynı kavram, üst yönetim tarafından, kurumun hedeflerine ulaşmasına yönelik, faaliyetlerin

raporlanması, yönetilmesi, izlenmesi maksadıyla oluşturulan süreçlerin bileşimi olarak da tanımlanmaktadır (IIA, 2017a, s.23; Aktaran, Gökdeniz, Kartal ve Yetiş 2017, s.65).

2.2 Risk

Türk Dil Kurumu (TDK) göre risk, zarara uğrama tehlikesi şeklinde tanımlanmıştır. İşletmeler açısından, gerçekleşme ihtimali olan bir olayın, gerçekleşmesi halinde kurumun amaç ve hedeflerinden sapmasına yol açabilecek olaylar olarak da ifade edilebilir. Çeşitli ulusal ve uluslararası standart ve çerçevelerde birbirinden farklı alternatif tanımlar bulunmaktadır. Her ne kadar risk'e ilişkin yapılan tanımlar ve çizilen kapsamlar birbirinden farklılık gösterse de tüm tanımların ortak paydası "risk" kavramının, belirsizlik ve sonuçlar ile yakın ilişki içerisinde görülmesidir. Buna göre; Risk, gerçekleştiği taktirde amaçlara erişilmesi hususunda olumlu ya da olumsuz etkisi bulunan belirsizliktir diyebiliriz. Belirsizlik ise, içerisinde fırsat ve tehdit barındıran bir olasılıktır. Riskin olumlu yanları ve sağlayabileceği olası kazançları fırsat, olumsuz yanları ve neden olabileceği olası kayıpları ise tehdit olarak ifade edilebilir.

İç denetimin tarihsel sürecine bakıldığında, sayım ve gözlem yoluyla değerlendirme yapılırken, bilgi, belge ve kayıtların artması üzerine örneklem usulüyle değerlendirilmeye geçilmiştir. Günümüzde ise iç denetim; organizasyon süreçlerindeki risklere odaklanmaktadır. (Ergin, Çetinoğlu ve Kurnaz 2008, s.19).

Artan rekabet koşullarıyla birlikte hızla değişen ekonomik koşullar karşında, kurumların mevcut durum değerlendirmelerinin yanı sıra, geleceği de öngörebilmeleri mühimdir. Kurumun belirlemiş olduğu amaç ve hedeflerine ulaşmasında doğru bilgi ve değerlendirmelere ihtiyaç duyulmaktadır. İç denetim bu noktada, uygulanabilir risk değerlendirme çıktılarını makul güvence ile yönetime sunmakla sorumludur (Bektaş U.C, 2019, s.65).

Geleneksel iç denetimde önceden belirlenen ölçütleri dikkate alarak ve rutinleşerek, mevcut sorunlara dikkat çekerek ilerlerken, denetimin yeniden şekillenmesiyle, iç denetim artık risk odaklı bir iç denetime dönüşmüştür (Ergin, Çetinoğlu ve Kurnaz 2008, s.19).

Risk odaklı iç denetim yaklaşımlarıyla riski odağına alan bir iç denetim;

bulunduğu organizasyon adına, değer katma misyonuyla stratejik risk temelli kurum kültürü yaratmak, değişimin hızını yakalamak ve dünya güncellerinin takipçisi olarak gelişmeleri proaktif çıktılarla ortaya koymaktadır. Teknolojik gelişmelerin hız kazanması ile büyük verinin, veri analitiğinin, yapay zekanın daha çok gündeme geldiği bugünün dijital dünyasında çarkın dişlilerinden olmaya devam edebilmesi için iç denetimin, değişimlere uyumu zaruridir. Aksi, çarkın dışında bırakır. Büyük veriden, analiz söz konusuyken teknoloji desteğiyle çıktı üretmek, hem iç denetim birimlerinin hem de organizasyonun avantajınadır. Bu nedenle yazılımsal çözümlerin organizasyonların tüm süreçlerine entegre edilmesi önemlidir.

Bu doğrultudaki verilerin elde edilmesi, artık dijital ortamlardan sağlansa ve kaynağına erişim kolaylaşsa da; verinin ölçülerek değer yaratma süreci hala bir o kadar karmaşıktır. Risklerin yönetiminin, olası bir kazayı önlemek veya suiistimali ortaya çıkarmak olmadığını düşünürsek, mevcut potansiyele değer katmanın optimizasyonu, büyük verinin ve komplike süreçlerin karşısında, güncel teknolojik gelişmelerin bünyeye dahil edilmeksizin insan eforuyla olamayacağı açıktır (Artius 2020, s.2).

Risk yönetim uygulamasıyla entegre çalışacak, organizasyondaki denetim prosedürlerine uyum konusunda denetim uzmanlarına yön verecek, denetimin etkinliğini artıracak bir GRC gibi bütüncül bir yazılıma ihtiyaç vardır. Böylelikle arkadan gelen bir denetim ve risk süreci modeli yerine, süreçlerle entegre bir denetim ve risk süreçleri otomasyonu sağlanması kritik öneme sahiptir.

2.3 Uyum

Bilindiği üzere, yasal düzenlemelere olan uyum, 2002 yılından bu yana özellikle ABD'de büyük önem kazanmıştı. İç denetçilerin çalışma usul ve esasları da bu dönem çıkarılan SOX Kanunu ile birlikte etkilenmiştir (Kaya 2015, s.170).

Özellikle küresel ölçekteki muhasebe skandalları sonrasında artan yasal düzenlemeler, gümrük işlemleri, ticari işbirlikleri ile anlaşmalardan doğan dış düzenlemeler ile kurum içi düzenlemeler, risk yönetimi ve yönetişimin geliştirilmesinde uyumluluk problemi ve günümüz işletme çevrelerinde önemli risk faktörleri olarak öne çıkmaktadır (Onay 2020, s.189).

Son zamanlarda yeni bir paradigma olarak, GRC kısaltmasıyla, yönetişim, risk ve uyum süreçlerinin bir arada bütünleşik bir yaklaşımla karşımıza çıkmaktadır. GRC yaklaşımı; süreç, strateji, teknoloji ve çalışan düzenlemesiyle işletmenin risk yaklaşımı, iç ve dış politika ve düzenlemelerle uyumlu bütüncül bir yaklaşımdır (Onay 2020, s.189).

2.4 Entegre GRC Kavramsal Model

İç Denetimde Yeni Trend olan GRC bir kuruluşun hedeflerine güvenle ulaşmasına, belirsizliğin kontrolünü eline almasına ve bütünlük içerisinde hareket etmesine olanak sağlayan entegre çözümler topluluğudur. GRC kısaltması ilk olarak 2003 yılında kullanılırken, konuyla ilgili ilk hakemli akademik makale 2007 yılında OCEG'nin kurucusu Scott L. Mitchell tarafından Uluslararası İfşa ve Yönetişim Dergisi (International Journal of Disclosure and Governance)'nde yayınlandı. Bu çığır açan makale, tüm yazılım ve hizmet endüstrisini etkiledi ve açık kaynaklı GRC standartlarının başlangıcı oldu (OCEG, s.1).

GRC, OCEG üyeliği tarafından, İlkeli Performans'a ulaşmak için bütünsel çalışması gereken kritik yetenekler olarak (performans, risk ve uyumluluk faaliyetlerinin yönetişimini, yönetimini ve güvencesini entegre eden yetenekler), iç denetim, uyumluluk, risk, hukuk, finans, BT, İK gibi departmanların yanı sıra iş kolları, yürütme ve yönetim kurulunun kendisi tarafından yapılan çalışmaları içermektedir (OCEG, s.1).

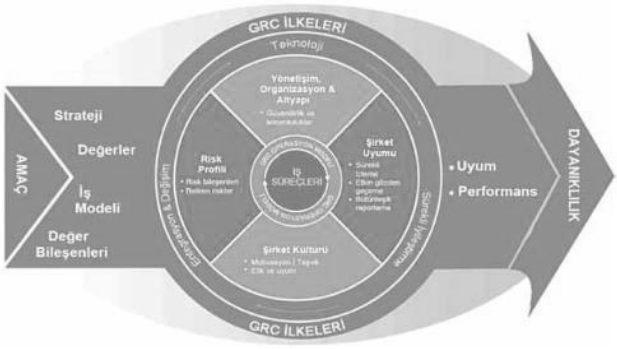
İlkeli Performans, kuruluşların hedeflerine güvenilir şekilde ulaşmasına, belirsizliği kontrol altında tutmasına bütüncül bir yaklaşımla hareket etmesine olanak sağlayan bir iş modelidir (Yalçınkaya, 2021, s.1). Hedef ilkeli performans elde etmekse, entegre GRC oraya ulaşmanın yoludur. GRC Yetenekleri, bir kuruluşun İlkeli Performans elde etmesine yardımcı, süreçler topluluğudur.

Kuruluşların risk ve uyumlulukları ayrı ayrı uzun zamandır yönetilmektedir bu bakımdan değerlendirildiğinde yeni değildir. Ancak kuruluşların bir çoğunda bu faaliyetlere olgun bir yaklaşım gösterilmemiş, iş süreçlerinin bütünlükle hareket etmesini sağlayan entegre çözümlere yönelik çabalar birbirini desteklememiştir. Bu nedenle örgütsel hedeflere ulaşma noktasında GRC modeli kritik rol oynadığı için devrimci niteliğindedir (Silva 2011, s.1).

GRC kapsamında ilk bilimsel tanım Racz vd. tarafından 2010 yılında yapılmıştır.

YRU; strateji, süreçler, teknoloji ve çalışanların düzenlenmesiyle işletmenin etik olarak doğru hareket etmesini ve risk yaklaşımı, iç politikalar ve dış düzenlemeler ile uyumlu olmasını sağlayan, böylece etkinliği ve verimliliği geliştiren işletme çapında yönetişim, risk yönetimi ve uygunluğu sağlamayı amaçlayan bütünleşik, bütüncül bir yaklaşımdır (Onay 2020, s.191).

GRC süreçleri; işletme faaliyetlerinin birçok alanını kapsar. KPMG'nin Bütünleşik Modeli (GRC Holistic Model); kişileri, verileri ve süreçleri bir araya getiren bütüncül bir çerçevedir. Bu model ile tüm GRC süreçlerinin koordinasyonun sağlanmasıyla, süreçleri yeniden düzenler ve gereksiz iş yükünün azaltılmasına yardımcı olur. Bu modele göre girdiler; iş süreçlerince işlenerek, uyum ve performans artışı olarak geri dönmektedir. Bir GRC sisteminde bulunan fonksiyon ve süreçler Şekil 1'de gösterilmiştir.



Şekil 1. GRC Bütünleşik Model (KPMG 2016, s.1)

Başarılı bir GRC için gerekli 8 faktör:

- Üst yönetim desteği
- İş süreçlerinde kişilerin aktif katılımı
- Mevzuat yükümlülüklerinin belirlenmesi
- Stratejik amaçların net bir şekilde ortaya konulması
- Risk değerlendirme yöntemlerinin belirlenmesi
- Değişiklik yönetiminin açık ve net biçimde tanımlanarak işletilmesi

• Kontrol ve uyum süreçlerinin faydaları bakımından farkındalık

• Kişilerin ve süreçlerin, teknolojilere uygunluğunun sağlanması

(KPMG 2016, s.2).

2.5 OCEG GRC Teorisi ve GRC Yetenek Modeli

Bu bölümde GRC uygulamalarına yön veren temel rehberleri yayınlayan OCEG teorilerine yer verilmiştir. 2002 yılında kurulan OCEG Amerika merkezli bir düşünce kuruluşudur. GRC alanında işletmelerin hedeflerine yönelik standart ve GRC dökümanlarını yayınlamaktadır. 2002 yılında OCEG tarafından GRC Capability Model (Red Book) ve sonraki yıllarda da GRC Assessment Tools (Burgundy Book) ve GRC Technology Solutions Guide yayınlanmıştır.

OCEG Red Book Bileşenler, aşağıda yayınlandığı şekilde sıralanmıştır (OCEG Red Book, 2012; Aktaran, Pehlivanlı 2015, s.131);

• C – Kültür ve İçerik

• O – Organize Etme ve Gözetleme

• A – Değerlendirme ve Sıralama

• P – Koruma ve Destekleme

• D – Tespit Etme ve Algılama

• R – Tepki Verme ve Çözme

• M – İzleme ve Ölçme

• I – Bilgi ve Entegrasyon

GRC Evrensel Çıktıları aşağıdaki gibidir (OCEG, Red Book, 2012; Aktaran, Pehlivanlı 2015, s.131);

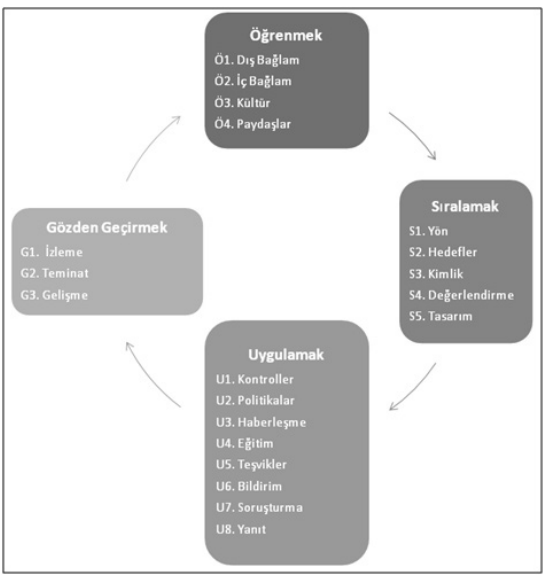
- Başarılı İş Hedefleri
- Organizasyonel Kültürü Geliştirme
- Pay sahiplerinin Güvenini Artırma
- Organizasyonu Hazırlama ve Koruma
- Sorunları Tespit Etme ve Kaçınma

- İstenilen Davranışa Motive ve Teşvik Etme
- Sorumluluk Geliştirme
- Ekonomik ve Sosyal Değeri Artırma

OCEG GRC Yetenek Modeli (Red Book); Yönetişim, risk, uyumluluk ve bilgi teknolojilerini bütünleşik bir yaklaşımda birleştiren ilk ve tek açık kaynak standardıdır. GRC profesyonellerinin İlkeli Performans elde edebilmesi için, GRC yeteneklerini planlamasına, geliştirmesine ve değerlendirmesine yardımcı olmaktadır.

Bir organizasyonun hedefleri doğrultusunda ilerlemesi, başarı için tek başına yeterli değildir. Bunun için, potansiyel riskleri, yasaları, sosyal adaleti ve belirsizliklerin sınırlarını da dikkate alınmalıdır. Risk yönetimi, uyum ve etik davranış da amacın ayrılmaz bir parçasıdır. Her bir iş sürecinin birbiriyle tam entegre şekilde yönetişim, risk yönetimi ve uyumluluk yetenekleri vasıtasıyla çalıştırılmalıdır (OCEG, s.1).

Şekil 2'de GRC Yetenek Modeli standardının bileşenleri gösterilmektedir.



Şekil 2. GRC Yetenek Modeli Bileşenleri (Yalçınkaya 2021, s.1)

3. GRC YAPILANMA SÜRECİ

3.1 Dijitalleşme

Dijitalleşme, bilginin sayısallaştırılması, sayısallaştırmanın ise ulaşılabilir olan analog bir bilgiyi, bilgisayar aracılığıyla dijital ortama aktarılması süreci olarak ifade edebiliriz (Karakaş vd, 2009; Aktaran, Özmen ve Ersöz 2020, s.172). Aynı zamanda dijital ortama aktarılan verilerden farklı sonuçlar ortaya çıkarma ve kuruma değer katma yönündeki dönüştürme süreci olduğunu söyleyebiliriz. Dijital dönüşümlerini tamamlamış olan şirketlerin, değişim ve yıkıcı teknolojik etkilerin karşısında, daha esnek, yalın ve hızlı yapılarıyla her türlü duruma karşı dayanıklı olacakları aşikardır (Kaya 2018, s.1).

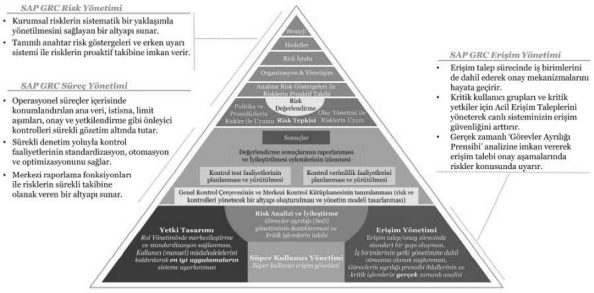
Dijital çağın yaşandığı günümüz koşullarında; işletmeler ayakta kalabilmek için çağın gereklerini yerine getirmek durumda kalmışlardır. Küreselleşmeyle birlikte, işletmelerin iş yapış biçimleri ve çevreleri değişmiştir. Dolayısıyla ulusal ve uluslararası çevrelerinin düzenlemelerine uyum sağlamakla yükümlü olmuşlardır. Bu yükümlülüklerin ise iyi bir uyumluluk yönetimi ile sağlanması mümkündür. Aynı zamanda ulusal ve uluslararası işletme çevreleriyle birlikte, rekabet ortamı da buna paralel artmış ve dış ticaretle birlikte değişen rekabet koşulları, işletmelerin risklerini de aynı ölçüde artırmıştır. Artan ve değişen risk faktörlerinin kontrol altında tutulabilmesi, etkin bir risk yönetimiyle mümkündür. Ulusal ve uluslararası faaliyette bulunan, işletme yöneticilerinin, hissedarlarının ve paydaşlarının haklarının korunması, etkin bir yönetişimi zorunlu kılmaktadır (Onay 2020, s.190).

Dijitalleşmenin veya dijital dönüşümün yalnızca ERP yazılımlarına geçiş, donanımsal yatırımlar veya diğer dijital teknolojilerin hayata geçirilmesi olarak algılanmaması, bunun aslında yeni bir kurumsal yapılanma modeli olarak tanımlanması gerektiğini, diğer yapılanmalardan farkının ise ‘’dijitalleşmeyi’’ merkezde tutarak bu yapılanmanın oluşturulmasına ve bunun ise diğer teknolojilerden daha geniş bir olgu olduğuna işaret etmiştir (Kaya 2018, s.1).

VUCA ve kriz dönemlerinde, şirketlerin denetim birimlerinden beklentilerinin artış göstermesi, denetçilerin teknolojik gelişmeleri bütünsel olarak ele alınması ihtiyacını da beraberinde getirmiştir. Dijital dönüşüm ve bilgi teknolojilerindeki değişimler, aynı zamanda işletmeleri, iş yapış biçimleri ve süreçleri bakımından da değişme zorlamaktadır (Bircan 2020, s.74).

3.2 GRC Yazılımları

GRC yazılımlarından bazıları; SAP GRC, Archer eGrc, Oracle, MetricStream, ACL şeklinde sıralanabilir. Bu yazılımların temel fonksiyonları dört başlıkta sıralanabilir; Risk Yönetimi, Süreç Yönetimi, Erişim Yönetimi, Denetim Yönetimi (Pehlivanlı 2015, s.168).



Şekil 3. GRC Yaşam Döngüsü (PWC 2011, s.1)

Bu bölümde Siber Güvenlik, Yönetim, Risk ve Uyumluluk bakımından entegre çözümleriyle öne çıkan SAP GRC yazılımı üzerinden değerlendirme yapılmıştır.

SAP GRC yazılımlarının işleyiş ve temel faydaları modül bazında aşağıdaki gibidir.

3.2.1 SAP GRC Risk Yönetimi (SAP GRC Risk Management | RM)

Güçlü bir kurumsal risk yönetimi için SAP GRC Risk Yönetimi ile riskleri tanımlama, değerlendirme ve izleme süreçlerinin etkinleştirilmesi, olası risk faktörlerinin analiz edilerek, mevcut ya da olası risklerin tanımlanarak sınıflandırılması, uygun önlemler alınması, ve kurumsal risk yönetiminin optimize edilmesi, risklerin sistematik bir şekilde ortadan kaldırılmasını sağlar (Felece s.1).

3.2.1.1 GRC Risk Yönetimi Temel Faydaları;

• Risk yönetimi silo yönetim yaklaşımından, yönetişim ve uyum ile koordineli çalışan bir yapıya kavuşmaktadır,

• İşletme için yüksek önem derecesinde olan riskleri konsolide edilmesi,

• Spesifik risklere odaklanıldığından, tüm işletmenin fonksiyonlarını ve ihtiyaçlarını dikkate alan bir risk yönetimini geliştirilmesini sağlar,

• Stratejik hedefler ve işletme hedeflerinin risklerle ilişkilendirilmesini ve karar alma sürecinde dikkate alınmasını sağlar,

• KRI-Anahtar Risk Göstergelerine paralel anahtar risklerin proaktif olarak izlenmesini sağlar (PWC 2011, Aktaran, Pehlivanlı, 2015, s.168-170).

3.2.2 SAP GRC Süreç Kontrolü (SAP GRC Process Control | PC)

Süreç ve uyumluluk yönetimlerini sistematik hale getirir, güvenli bir iç kontrol programı ile sürekli kontrol ve izleme faaliyetleriyle test süreçlerini kolaylaştırır, temel sorunlara gerçek zamanlı bilgilerle riskleri azaltarak tüm iş süreçlerinde kapsamlı kontrol sağlar, ve sistemin sektöre özel tüm prosedürlerine uygunluğunu sağlar (Felece s.2).

3.2.2.1 GRC Süreç Yönetimi Temel Faydaları;

• Manuel kontrollerin otomasyona imkan vermesi

• Kontrollerin hedeflendiği amaç üzerine optimizasyonu sağlar

• Kontrollerin testi ve dökümantasyonu, merkezi raporlama altyapısıyla sağlanması

• Merkezi çoklu uyum çerçevesinin süreçlerle bütünleştirilmesi

• Sürekli gözlem altyapısının sağlanması

• Kontrol testleri standart, insiyatif almadan, sistematik ve süreklilik mantığıyla yürütülür

• Bütünleşmeyi sağladığından iç ve dış denetim maliyetlerini azaltır (PWC 2011, Aktaran, Pehlivanlı, 2015, s.168-170).

3.2.3 SAP GRC Erişim Kontrolü (SAP GRC Access Control | AC)

Erişim ihlalleri riskini hızlıca tespit ederek ortadan kaldırır, şirket içi uygulamalar ve verilerin erişimin yönetilebileceği teknolojik altyapıyı oluşturur, Risk yönetimi sürecini şeffaflaştırarak, maliyetlerini düşürür.

Kullanıcı ve uygulamaları, risklerin sürekli izlenebilmesini sağlayarak, kullanıcı yetkilendirmesi, yetki dağılımı ve ayrıcalıklı erişim süreçlerini otomatikleştirilmesini sağlar. Önleyici denetimlerle, acil durum erişimini izleyebilir ve uyum kontrolüyle risk azaltımı iş süreçlerine entegre edilebilir (Felece s.2).

3.2.3.1 GRC Erişim Yönetiminin Temel Faydaları;

• Görevlerin ayrılığı ilkesine uyumların gerçek zamanlı izlenebilmesi,

• Erişim risklerinin izlenebilmesi ve bu risklere karşı önleyici kontrollerin devreye alınması,

• Sistemdeki kullanıcı ve erişimler izlenebilir,

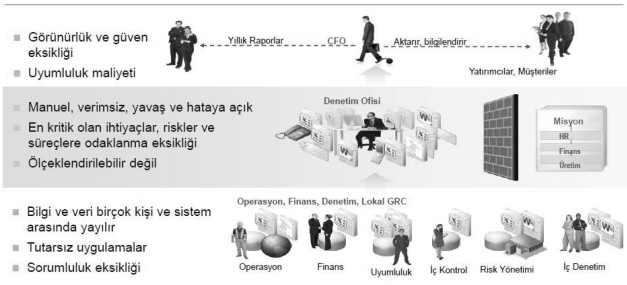
• Merkezileşmiş denetim dökümantasyonu yürütülebilir,

• Önleyici kontrol mekanizmaları,

• Görevlerin ayrılığı ilkesinin değerlendirilmesini imkan tanır (PWC, 2011, Aktaran, Pehlivanlı, 2015, s.168-170).

3.2.4 SAP GRC Denetim Yönetimi (SAP GRC Audit Management | AM)

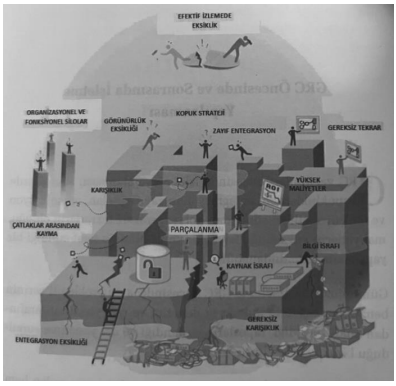
İç denetim plan ve prosedürlerini otomatikleştirerek, denetim raporu, kanıt toplama, elektronik çalışma kağıtlarının oluşturulması gibi iç denetim aktiviteleri basitleştirilebilir. Güvenilir içgörüler edinilmesini sağlayarak iş süreçlerindeki kritik risk ve kontrollerle uyumlu hale getirilebilir (Felece s.2). GRC teknolojik çözümlerin uygulanmadığı durumlarda kontrol ve uyumluluk yönetimindeki zorluklar aşağıdaki gibidir;



Şekil 4. GRC Dışı Kontrol ve Uyumluluk Yönetimindeki Zorluklar (Akaltan & Edebali 2014, s.6)

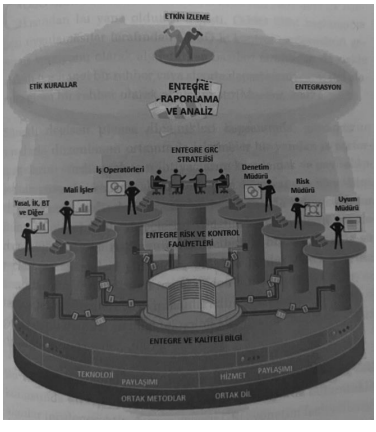
3.3 GRC Öncesinde Ve Sonrasında İşletme Yapılanması

GRC yazılımları öncesinde işletme yapılanmalarını; Strateji kopuklukları, entegrasyon zayıflıkları ve organizasyonların fonksiyonelliklerin de silo yönetimlerinden kaynaklı gereksiz tekrarların olması ile maliyetlerin arttığı, bilgi ve kaynak israfının yükseldiği bir yapı şeklinde tanımlanabilir. Günümüzde GRC çözümlerinden faydalanmayan işletmeler, aynı problemi benzer gerekçelerle uyumluluk, iç denetim ve risk yönetimi tarafından analiz edilip üst yönetime raporlandığı bir çalışma kültürü hakimdir. Süreçlerin kendini gereksiz tekrar etmesi hem bütçe hem de gereksiz iş yükü ve süreç yöneticileri bakımından motivasyon kaybı ile müşteriye yansımaları söz konusu olmaktadır (Pehlivanlı, 2015, s.91).



Şekil 5. GRC Öncesi Yapılanma (Pehlivanlı, 2015, s.92)

Yukarıda şekilde görülen tablo, günümüz işletme faaliyetlerinin bir çoğundaki kısır döngüyü göstermektedir.



Şekil 6. GRC Sonrası Yapılanma (Pehlivanlı, 2015, s.92)

GRC ile birlikte işletmelerde denetim, iç kontrol, risk yönetimi gibi organizasyonların etkinliklerinin artacağı, maliyetlerinin azalacağı, dolayısıyla işletmelein risk yönetimini daha aktif kullannabilecekleri şeklinde yorumlanabilir.

3.4 GRC Öncesinde Ve Sonrasında İç Denetim Yapılanması

İç Denetçilerin değişen Dünya koşullarıyla uyumlu bir şekilde çalışmalarını sürdürebilmeleri için, IIA iç denetimin tanımını, mesleğin kapsamını, standartlarını, teknolojik ve bilimsel gelişmeleri, paydaşların ihtiyaç ve beklentilerini, iç denetçilerin görev, yetki ve sorumluluk düzeyinde bir bütün olarak yeniden gözden geçirmesine neden olmuştur. 1950'li yıllarından beri mesleğin kapsamını, gerek gördüğü periyotlar da yeniden güncellemiştir (Onay 2020, s.189). İç denetimin güncel tanımı ile uluslararası standartlarına bakıldığında, mesleğin odağında risk yönetimi ve yönetişim faaliyetleri olduğu görülmektedir.

Sürekli değişim ve dönüşüm içerisinde olan küresel dinamiklerin karşısında, öncelikle iç denetimin kendisi başta olmak üzere, yeni koşullara göre köklü bir değişim ve dönüşümü zorunlu kılmıştır (Bircan 2020, s.69). Denetim metodolojisinden ve standartların yeniden gözden geçirilmesine kadar etkileyen dijital dönüşüm, işletmelerin tüm süreçlerindeki, iş yapış biçimlerini yüksek oranda etkilemektedir. Dolayısıyla bu değişim karşısında, geleneksel iç denetim anlayışıyla ve klasik yöntemlerle yetinilmesi mümkün olmayacaktır.

Geleneksel denetim yaklaşımlarında, organizasyonun mali hesapları, yasal mevzuata uygunluğu, maddi doğruluğuyla ilgili makul güvenceye odaklanılmıştır. Tarihsel sürece bakıldığında, küreselleşme ve teknolojik gelişmelere bağlı olarak denetiminde sürekli bir dönüşüm içerisinde olduğu gözlemlenmektedir. Dijital dünyadaki gelişmelere bakıldığında denetiminde bu gelişmelerle uyum içinde olması zorunluluk haline gelmiştir (Köse ve Polat 2021, s.11).

Denetim alanında oluşan yeni dinamiklerle, değişen ihtiyaçları mevcut denetim prosedürleriyle karşılamak mümkün görünmediği için denetimin etkin yürütülmesi, paydaşların ihtiyaçlarını karşılaması ve olması gereken makul güvenceyi sağlayabilmesi için teknolojik çözümlerin tüm süreçlerinde uygulaması gerekir.

Geleneksel iç denetim anlayışından risk odaklı denetim anlayışına evrilen iç denetim, geçmişe yönelik tespitten ve sonradan alınan aksiyonlardan, kuruma değer katan yaklaşımlarla, riskleri önceden değerlendiren gelecek odaklı denetim anlayışına dönüşmüştür.

İç denetçilere yönelik IIA'in standartları kapsamında, bilgi teknolojileri süreçlerinde uymaları gereken, bazı yükümlülükler getirilmiştir. İç denetçilerin yükümlülüklerine ilişkin, standartlar incelendiğinde; yönetişim, risk yönetimi ve kontrol başlıklarıyla aşağıdaki hususlar öne çıkmaktadır:

• İç denetim birimlerinin, işletmelerin hedef ve stratejilerine yönelik bilgi teknolojileri ve yönetişimin değerlendirilmesi,

• BT risklerinin değerlendirilmesinden iç denetim birimlerinin sorumlu olması,

• BT risklerine karşı, kontrollerin yeterliliği ve etkinliğinin değerlendirilmesinden, iç denetim birimlerinin sorumlu olması (Çakalı ve Baloğlu 2022, s.3).

Yönetişim, Risk ve Uyum yönetimi birbirleriyle ilişkili olması sebebiyle bütüncül bir yaklaşım modeli olarak ele alınmıştır. Bütünsel yaklaşım olarak ele alınmasının tarihsel geçmişi on yıl gibi bir süreyi kapsamaktadır ve oluşan farkındalık giderek artmaktadır.

İç denetim, GRC süreçlerini bağımsız ve objektif değerlendirmeye tabi tutarak işletmenin hedeflerine ulaşıp ulaşmayacağına dair yönetime makul bir güvence vermektedir. İç denetçiler bunun için işletmenin risk alanlarını, risklerini izleme etkinliğini ve tanımlanan risklere karşı sorumluluklarının yeterliliğini dikkate alır ve yönetişim risk, uyum kontrollerinde sistematik bir yaklaşımla değerlendirir (Pehlivanlı 2015, s.103).

GRC, entegrasyon ile bütünleştirme yoluyla risk, kontrol ve denetim maliyetlerini düşürerek etkinliğini artırmakta. GRC entegrasyonunun amacı, risk, kontrol ve bulguların aynı şekilde sınıflandırılması da dahil olmak üzere iş süreçlerinin tamamı arasındaki geleneksel sınırlılıkları ortadan kaldırarak bölünmüş bir yapı yerine tek bir risk yaklaşımı geliştirmektir (KPMG 2016, s.1).

3.5 GRC'nin Denetimdeki Kritik Rolü

GRC süreci, organizasyon süreçlerinin stratejik hedef yönünde yaşamsal döngüyü sağlarken etkin olmalıdır. Entegre çözüm yaklaşımıyla iç denetim, insan kaynakları, finans, yasal prosedürler, üretim, bilgi teknolojileri ve pay sahiplerini aynı amaç etrafında toplar (Pehlivanlı 2015, s.103).

Kurumların mevcut risk yönetim ve denetim süreçlerinin, dijital dönüşüme uyarlanarak, süreçlerinde işlevsellik kazandırılması halinde sonuçlar kısaca aşağıdaki gibidir;

• Büyük verinin analiz edilebilmesi,

• Örneklem yoluyla sonradan yapılan denetim ve risk analizi yerine, organizasyonun tüm süreçlerinin bütünsel denetim mekanizmalarıyla sürekli denetlenmesinin sağlanabilmesi

• Operasyonlarında, yazılımsal çözümlerden yararlanılmasıyla, kaydı olmayan her bir verinin de sistemde artık ayaz izi var demektir. Buda sistemde kayıt dışı bırakılan verinin de izi sürülebilir anlamına gelir. Ancak her ne kadar verinin sisteme dahil edilmesi bakımından kayıp ve kaçağın yazılım desteğiyle önüne geçilmiş olsa da, hala bu büyük veriyi konsolide ederek değer üretebilecek bir insan eforu pek yok. Olduğu varsayımından yola çıkarsak bile, riskin meydana gelmesi halinde derhal bir aksiyona geçerek değer yaratmaya dönüştürmesi noktasında zaman çok önemli bir kavram haline gelmektir. Dolayısıyla güncel teknolojik yaklaşımlarla desteklenmiş bir iç denetçi kilit noktadır.

• Riskler gerek nitel gerekse nicel yöntemlerle analiz edilse de tek akıl ve prosedür tarafından konsolide edilmedikçe, risklerin objektif değerlendirilemeyeceği bunun da ek maliyetlere sebep olmaya devam edebileceği,

• Silo yönetiminin söz konusu olduğu organizasyonlardaki risklerin; merkezi stratejilerle risklerin eşleştirmesinin imkansızlaşması, ve aynı eforun tekrar tekrar sarf edilerek hem zaman hem de para kaybına sebep olmaya devam etmesi,

• Büyük ve karmaşık olan veriden anlamlı sonuçlar çıkarılmasının önemli olduğu kadar kurumun risk hafızasının olması ve risklerin onaylanmış bir risk yaklaşımıyla yönetilebilmesi bakımından, risk yönetimi yazılımı kullanılması

da bir o kadar önemlidir. Risklerin tespitiyle birlikte bütünsel yaklaşımıyla GRC teknolojik çözüm modeli, strateji temelli risk yönetimi de iç denetimin yükselen trendi olmuştur. Buna paralel denetimin kritik önemi de artmaya devam etmektedir (Artius 2020, s.2).

4. SONUÇ

Şirketlerin büyümesi ile artan rekabet ortamı ve yeni nesil teknolojilerin gelişmesiyle kurumların erişim sağladıkları veri miktarları da her geçen gün artmaya devam etmektedir. Bu artış, aynı zamanda kontrol mekanizmalarının karmaşıklığını da beraberinde getirirken veri güvenliği riskini de ortaya çıkarmaktadır. Tabi tüm bunların yanı sıra değişen ve dönüşen küresel ekonomiyle birlikte genişleyen iş çevreleri ulusal ve uluslararası paydaşlar nezdinde uyulması gereken yasa, mevzuat ve yükümlülükler de öne çıkan önemlilikler arasındadır. GRC gibi yeni nesil teknolojik çözümlerle, GRC ile entegre süreçlerin otomasyonunun sağlanması, GRC risk yönetimini etkin bir kontrol mekanizmasıyla güvenli şekilde yapılabilmesi vuca döneminin yaşandığı günümüz koşullarında kurumlar için hayati öneme sahiptir. Tamda bu nokta da GRC teknolojik çözümleri, kurumsal risklerin sistematik bir yaklaşımla yönetilmesi, belirsizliği güvenli şekilde kontrol altına almayı sağlayan altyapıyı sunar. Tüm işletme süreçleri birbirleriyle etkileşimde ve tam entegre tasarlandığı için süreç yönetimi, denetim yönetimi, yönetişim gibi modülleriyle de bağlantı kurarak riskleri ilgili süreç kontrolleri ile eşleştirir, hızlı aksiyona olanak sağlar.

KAYNAKÇA

AlexInformation, Risk Based Auditing ,Alexbanking, Las cimas, Suite 300, Ausitin,2005.

Akaltan N. ve Edebali M. (2014).Doğru Taktik GRC, Sap Innovatıon Forum, s.6

Artius (2020). *Risk Yönetiminin Dijital Dönüşümü.* Erişim Adresi: https://www.artius.com.tr/blog/risk yonetiminin-dijital-donusumu-bolum-ii.php . Erişim Tarihi: 10.06.2022.

Bircan N.G. (2020). İç Denetimde Yapısal Değişim ve Dönüşüm: İç Denetçilerin Farkındalığı ve Beklentileri Üzerine Bir Araştırma, *Muhasebe Enstitüsü Dergisi,* 63, 67-83

Bektaş U.C.(2019) *Uluslararası İç Denetim Standartları Çerçevesinde Risk Odaklı İç Denetim Ve Uygulamaya Yönelik Bir Araştırma,* (Yayımlanmamış Yüksek Lisans Tezi), Ufuk Üniversitesi, Ankara

Çakalı K.R.ve Baloğlu G. (2022). Bilgi Teknolojileri Yönetişiminin Denetimi. *Denetim ve Güvence Hizmetleri Dergisi* 2(1).

Ergin H. , Çetinoğlu T. ve Kurnaz N. (2008). Risk Odaklı İç Denetim: Türkiye'nin 500 Büyük Sanayi İşletmesinde Ampirik Bir Değerlendirme. *Muhasebe ve Denetime Bakış,* (26), 17-36 .

Ersöz B. , Özmen M. (2020). Dijitalleşme ve Bilişim Teknolojilerinin Çalışanlar Üzerindeki Etkileri, *Bilişim Teknolojileri Online Dergisi,* 11 (42), 171-179.

Erturan İ. , Ergin E. (2018). Dijital Denetim Ve Dijital İkiz Yöntemi, *Muhasebe Bilim Dünyası Dergisi,* 20(4), 810-830

Fidan Y. (2011). Yönetimden Yönetişime: Kavramsal Bir Bakış, Yalova *Sosyal Bilimler Dergisi,* 1, 5-10.

Felece. SAP Siber Güvenlik, Yönetim, Risk ve Uyumluluk, Erişim Adresi: https://www.felece.com/solutions/sap-siber-guvenlik-yonetim-risk-ve-uyumluluk Erişim Tarihi: 18.06.2022.

Gökdeniz, İ. , Kartal, C. ve Yetiş, Ö. (2017). Kurumsal Yönetim Amaçlarına Ulaşmak İçin Yönetim Modeli: Kurumsal Öğrenmeyi Destekleyen İç Denetim, *Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* 4 (3) , 64-80.

DOI: 10. 30803/adusobed.317960

IIA. (2022). Definition of Internal Auditing. Erişim Adresi: www.theiia.org https://www.theiia.org/en/standards/what-are-the-standards/mandatory guidance/definition-of-internal-audit/ . Erişim Tarihi: 29.05.2022.

Köse H.Ö, Polat N (2021). Dijital Dönüşüm ve Denetimin Geleceğine Etkisi, Sayıştay Dergisi, 123, 9-41.

Kaya B.(2015). *İç Denetim, İç Kontrol ve Risk Yönetimi,* Ankara : Yaklaşım

KPMG. (2016). Yönetişim Hizmetler: GRC: Yüksek Performans ve Düşük Maliyet için Ortak Dil, Erişim Adresi: https://assets.kpmg/content/dam/kpmg/pdf/2016/05/IRM-Yonetisim-4-GRC.pdf. Erişim Tarihi: 18.06.2022.

KPMG (2016). GRC Gündemi, Erişim Adresi:https://assets.kpmg/content/dam/kpmg/pdf/2016/04/tr grc-magazine-24feb.pdf . Erişim Tarihi: 12.06.2022.

Kaya B. Dijital Dönüşümde İç Denetçilerin Rol ve Sorumlulukları. Erişim Adresi: https://bertankaya.net/2018/06/dijital-donusumde-ic-denetcilerin-rol-ve-sorumluluklari/. Erişim Tarihi: 09.06.2022.

Mira da Silva, M.. (2011). A Conceptual Model for Integrated Governance, Risk and Compliance. 6741. 199-213. 10.1007/978-3-642-21640-4_16.

Onay A, (2020). Yönetişim, Risk, Uygunluk (YRU) Yaklaşımı Açısından İç Denetim Fonksiyonunun Sorumlulukları ve İlişkili Taraflara İlişkin Bir Araştırma, *Muhasebe ve Denetime Bakış Dergisi,* 59, 187-212.

OCEG. Governance-Risk-Compliance (GRC). Erişim adresi: https://www.oceg.org/about/what-is-grc/. Erişim Tarihi: 12.06.2022.

OCEG. GRC Capability Model (Red Book). Erişim adresi: https://go.oceg.org/grc-capability-model red-book. Erişim Tarihi: 12.06.2022.

Pehlivanlı D, (2015). *Yönetişim, Risk ve Uyum,* İstanbul : Beta Basım Yayım,

PWC (2011). GRC Yaşam Döngüsü. Erişim adresi: https://www.pwc.com.tr/tr/hizmetlerimiz/risk surec-teknoloji-hizmetleri/erp-risk-hizmetleri/ic-denetim-analitigi/yonetisim-risk-ve-uyum-cozumleri.html. Erişim Tarihi: 12.05.2022.

Yalçınkaya S.G (2021). Governance, Risk Management and Compliance (GRC–

Yönetişim, Risk Yönetimi ve Uyum) ve GRC Yetenek Modeli Standardı. Erişim adresi: https://www.siberkavram.com/2021/06/governance-risk-management-and.html. Erişim Tarihi: 12.06.2022.