Muhasebe ve Finansman Dergisi – Ocak 2022 (93): 31- 52

ISSN: 2146-3042
DOI:

Kurumsal Risk Yönetimi ve Bulut Bilişim Sistemi*

Hüseyin ÖZYİĞİT**

ÖZET

Bulut bilişim sistemi; bir işletmenin veya kuruluşun bilgi işlem kaynaklarını ve uygulamalarını herhangi bir konumdan, internet bağlantısı aracılığıyla temin etmesini sağlayan tedarik modelidir. Ayrıca, işletme organizasyonlarının; iş modeli yeteneklerini ve bilgi işlem kaynağı taleplerini potansiyel olarak artırmalarına ve geliştirmelerine olanak tanımaktadır. Bu çalışmanın amacı; bulut bilişim sistemini COSO'nun (Committee of Sponsoring Organizations of the Treadway Commission) kurumsal risk yönetimi ilkeleriyle bağdaştırarak, bulut bilişim sisteminin işletmeler üzerindeki risklerini ve etkisini özlü bir şekilde ortaya koymaktır. Sonuç olarak işletme yöneticilerinin kurumsal risk yönetimi odaklı bulut bilişim sistemi sorumlulukları belirtilerek; bulut bilişim sisteminin COSO kurumsal risk yönetimi çerçevesi paralelinde kullanıldığında işletmelere fayda sağlayacağı ve işletme yöneticilerinin bulut bilişim sistemini kullanarak, karşılaşabilecekleri riskleri daha detaylı ve kapsamlı değerlendirmelerine yardımcı olacağı öngörülmektedir.

Anahtar Kelimeler: *Kurumsal Risk Yönetimi, Bulut Bilişim Sistemi.*

JEL Sınıflandırması: *G3, M10, O32.*

Enterprise Risk Management and Cloud Computing System

ABSTRACT

A Cloud computing system is a procurement model that enables a business or organization to procure computing resources and applications from any location, via an internet connection. In addition, it also allows business organizations to potentially increase and develop their business model capabilities and computing resource demands. The aim of this study is to concisely present the risks and impact of cloud computing systems on businesses by associating cloud computing systems with COSO's enterprise risk management principles. As a result, it is foreseen that the cloud computing system will benefit businesses when used in parallel with the COSO enterprise risk management framework, by specifying the enterprise risk management-focused cloud computing system responsibilities of business managers, and it will help business managers to evaluate the risks they may face in more detail and comprehensively by using the cloud computing system.

Keywords: *Enterprise Risk Management, Cloud Computing System.*

JEl Classification*: G3, M10, O32.*

* **Makale Gönderim Tarihi:** 21.10.2021, **Makale Kabul Tarihi:** 10.12.2021, **Makale Türü:** Kuramsal

** Dr. Öğr. Üyesi, Erzincan Binali Yıldırım Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, huseyinozyigit@erzincan.edu.tr, ORCID: 0000-0002-0632-7931.

1. GİRİŞ

Bilgi işlem teknolojisinin gelişim sürecinde; genel bilgisayarlardan kişisel bilgisayarlara, sunucu merkezli sistemlerden "Web" sayfalarına geçiş yapılmıştır. Günümüzde birçok işletme; teknoloji ve iş ortaklığından sonraki en önemli dönüm noktasını "Bulut Bilişim Sistemi" olarak görmektedir. İnternet üzerinden gerçekleştirilen ve depolanan hizmetlerin detaylı, kapsamlı ve alternatifli versiyonu olan bulut bilişim, işletme organizasyonlarının; altyapı, eğitim, personel ve yazılım yatırımlarından ziyade iş modeli yeteneklerini ve bilgi işlem kaynağı taleplerini potansiyel olarak artırmalarına ve geliştirmelerine olanak tanımaktadır. Sistem sanallaştırma, sistem kaynak yönetimi ve internetteki teknolojik gelişmeler; birçok işletmenin teknoloji ihtiyaçlarını karşılamak için bulut bilişim sisteminin alternatif olarak ortaya çıkmasına sebep olmuştur. Bulut bilişim sisteminin işletme yöneticilerine sunduğu temel avantajlar (COSO, 2012: 1);

- Bilgi işlem faaliyetlerinin anlık olarak işlenmesi ve komutlarının yerine getirilmesi,
- Daha düşük maliyetlerle teknoloji harcamalarından daha fazla verim sağlanması,
- Standardizasyonu kolaylaştırabilecek ortak teknoloji platformlarının oluşturulması ve
- Teknoloji personeline olan ihtiyacın azalması şeklinde sıralanabilir.

Bulut bilişim sistemi işletmelere; iş birliği, etkileşim, kurumsal bağımlılıklar, daha hızlı kaynak bilgi sağlama ve farklı iş modelleri gibi birçok yenilik katmaktadır. Bu yeniliklerin etkin ve eksiksiz bir şekilde sürdürülmesi bulut bilişimin verimliliğini arttırmaktadır. Aksi bir durumda bulut bilişim için risk unsuru taşımaktadırlar. COSO işletmelerin risklerini, bütünsel bir bakış açısıyla değerlendirmek ve denetlemek için ortak bir dil ve temel oluşturmaktadır. COSO'ya göre "Kurumsal Risk Yönetimi-KRY", işletme yönetiminin belirsizlik, risk ve fırsatlarla etkin bir şekilde başa çıkmasını sağlayarak işletmelerin değer oluşturma kapasitesini arttırmaktadır. Ayrıca COSO'nun kurumsal risk yönetimi çerçevesinde belirtildiği üzere; önemli fırsatların, belirsizliklerin ve risklerin tanımlanması ve değerlendirilmesi; bulut bilişim paradigması aracılığıyla işletim ortamında daha hızlı ve kolay olacaktır.

Çalışmada; bulut bilişim sistemini COSO'nun kurumsal risk yönetimi ilkeleriyle bağdaştırarak, işletmeler üzerindeki risklerini ve etkisini özlü bir şekilde ortaya koymak amaçlanmıştır. Üst düzey işletme yöneticileri; bulut bilişimin riskleri ve faydaları hakkında ne kadar eğitimli ve bilgili olurlarsa, işletmelerini geleceğe o kadar etkili bir şekilde hazırlayabilecekleri öngörülmektedir. Ayrıca bu çalışmanın; işletme yöneticilerinin, ortaya çıkan riskleri daha detaylı ve kapsamlı tanımlamasına, izlemesine, azaltmasına veya kabul etmesine olanak sağlayacağı düşünülmektedir.

2. LİTERATÜR TARAMASI

Araştırmayla ilgili olarak kurumsal risk yönetimi ve bulut bilişim sistemi üzerine yapılan çalışmalar incelenerek kronolojik sıra ile sunulmuştur. PwC (2004), anket yöntemini kullanarak yönetim kurulu başkanlarının risk ve risk yönetimi ile ilgili görüşlerini araştırmıştır. Yönetim kurulu başkanlarının yaklaşık %50'sinin mevcut riskleri belirlediklerini, ölçtüklerini ve yönettiklerini tespit etmiştir. Anket sonuçlarına göre yönetim kurulu başkanlarının %23'ü risk yönetimi için ortak bir görüşe ve birtakım standartlara sahip olduklarını belirtirken yine yönetim kurulu başkanlarının %26'sı tüm kurum çapında risk

yönetimi için gerekli bilgilere ve verilere sahip olduklarından emin olduklarını iddia etmiştir. Desender (2007) çalışmasında, işletme yönetim kurulu ile kurumsal risk yönetimi arasındaki ilişkiyi araştırmıştır. Yönetim kurulu başkanının, yönetim kurulundaki konumuna göre kurumsal risk yönetiminde önemli bir etkiye sahip olduğunu ve yönetim kurulunun, yönetim kurulu başkanının bağımsızlığının kurumsal risk yönetiminin etkinliğini artırdığını tespit etmiştir.

Marsh (2008), New York'ta Uluslararası Finansal Yöneticiler (Financial Executives International- FEI) ve Risk ve Sigorta Yönetimi Topluluğu (Risk and Insurance Management Society-RIMS) ile yaptığı araştırmada; kurumsal risk yönetimini yeterli derecede dikkate almasa dahi, her altı yöneticiden dördünün risklere karşı daha kurumsal bir bakış açısıyla yaklaşılması gerektiğini düşündüğü ve sadece on yöneticiden ikisinin bunu gerçekleştirebildiğini tespit etmiştir. Deloitte (2009), aktif büyüklükleri 19 milyon dolar olan bireysel ve ticari bankalar ile diğer finansal kuruluşlardan 111 tanesine anket uygulamıştır. Anket sonucuna göre risk yönetim departmanlarının; %15'inin risk komitesine, %15'inin finansal işler müdürüne, %52'sinin yönetim kuruluna, %78'inin ise denetim komitesine veya risk komitesine veya yönetim kurulu başkanına raporlama yaptıkları tespit edilmiştir.

Oriol ve Jordi (2010), risk yönetim prosedürlerinin bulut bilişim sistemine dahil edilmesini araştırmışlardır. Bulut bilişim risk yönetimi yaklaşımıyla, iş hedeflerinin gerçekleştirilme olasılığını artırabilen ve bu hedeflere yönelik riskleri kontrol altına alan bulut hizmet sağlayıcıların olduğunu tespit etmişlerdir. Shigeaki ve diğerleri (2011), işletmelerin bulut bilişimi kullanırken karşılaşabilecekleri riskleri incelemiş ve risk faktörlerini, kapsamlı bir şekilde analiz edip değerlendirmişlerdir. Sonuç olarak genel bulut kullanımını teşvik etmek, rekabet gücünü artırmak, işletim maliyetlerini azaltmak ve kurumsal yönetim verimliliğini yükseltmek için önlem ve önerilerde bulunmuşlardır.

Grace ve diğerleri (2015), kurumsal risk yönetiminin maliyet ve gelir etkinliğine etkisini test etmişlerdir. Çalışmada veri zarflama analizi ile etkinlik sıfırdan bire kadar ölçümlenerek firmaların karşılaştırılması sağlanmıştır. Daha sonra yapılan çoklu regresyon analizinde kurumsal risk yönetimi uygulamalarının maliyet ve gelir etkinliğinde ekonomik ve istatistiksel olarak önemli artışlar sağladığı görülmüştür. Abdelrafe ve diğerleri (2016) çalışmalarında, bankacılık faaliyetlerine yönelik bulut bilişim sisteminde risk yönetimi için yeni bir kavramsal çerçeve modellemesi önermiştir. Bankacılık organizasyonunda başarılı bir bulut bilgi işlem çerçevesini oluşturmak için bulut bankacılık uygulamaları, bulut hizmet modelleri, bulut dağıtım modelleri, bulut risk yönetimi modelleri ve bulut güvenlik modelleri gibi beş ana aşama belirlemişlerdir.

Samer ve diğerleri (2017), risk yönetim süreçlerini bulut bilişime uygulamak için kavramsal bir model önermişlerdir. Bulut bilişim ağlarını oluşturmak amacıyla veri ve bilgilerin uygun şekilde korunmasını sağlamak için risk yönetiminin farklı süreçlerini (risk tanımlama, risk analizi, risk planlama, risk yürütme ve risk izleme) ve bu süreçlerin bulut bilişim sistemini nasıl etkileyebileceğine dair önerilerde bulunmuşlardır. Ciğer ve Kınay (2018), nitel araştırma yöntemlerinden yarı yapılandırılmış görüşme tekniğini kullanarak Antalya ilinde faaliyet gösteren bağımsız denetim firmalarının bulut bilişim teknolojilerini benimseme düzeylerini araştırmışlardır. Altı bağımsız denetim firması ile görüşme gerçekleştirilmiştir. Sonuç olarak, denetim firmalarının bulut bilişim uygulamalarını tercih

etme nedenlerinin büyük boyutlu dosyaların gönderilmesi ve verilerin güvende tutulması olduğu tespit edilmiştir.

Yavuz ve Özyiğit (2018) tarafından yapılan çalışmada; çoklu doğrusal regresyon yöntemi kullanılarak, kurumsal risk yönetimi sisteminin bankaların performansı üzerindeki etkisi araştırılmıştır. Sonuç olarak; kurumsal risk yönetimi sistemi ile bankaların performansı arasında olumlu bir ilişki olduğu ve kurumsal risk yönetimi sisteminin bankaların performansını arttırdığı tespit edilmiştir. Akbaba (2019) çalışmasında; bulut muhasebe kavramına, bulut muhasebenin tercih edilme yoğunluğuna ve işletmeler için avantaj ve dezavantajlarına değinmiştir. Literatür incelenerek, bulut bilişim ve bulut muhasebenin işletmelerde uygulanma oranına ve teori ile uygulamada yapılması gereken muhasebe işlemlerine yönelik bilgiler verilerek önerilerde bulunmuştur.

Erdem (2020) çalışmasında, Finansal Muhasebe Standartları Kurulu (Financial Accounting Standards Board-FASB) tarafından yayınlanan "Bulut Bilişim Hizmet Anlaşmaları İle İlgili Oluşan Uygulama Maliyetlerinin, Müşteri İşletme Tarafından Muhasebeleştirilmesi" başlıklı standardı detaylıca inceleyerek, Uluslararası Finansal Raporlama Standartları'nda yapılabilecek değişikliklere ilişkin güncel bir bakış açısı sunmuştur. Özyiğit (2021) çalışmasında, işletmelerin bağımsız denetim odaklı kurumsal risk yönetimi sistemini oluşturmalarına yönelik araştırma yapmış, sözel model yöntemini kullanarak model geliştirmiştir. Modelde yedi ana aşama ve bu ana aşamalara ait alt aşamalar oluşturulmuştur. Geliştirilen modelin aşamalarına yönelik detaylı açıklamalar yaparak önerilerde bulunmuştur.

Literatür taraması değerlendirildiğinde; kurumsal risk yönetimi sistemi üzerine yapılan çalışmaların denetim, firma performansı, farkındalık, yönetimsel ilişki ve risklerin yönetilmesi konularına yönelik olduğu, bulut bilişim sistemi üzerine yapılan çalışmaların ise muhasebe standartları, muhasebe kayıtları, denetim firmaları, risk yönetim süreçleri ve bankacılık faaliyetlerine yönelik olduğu tespit edilmiştir. Kurumsal risk yönetimi ve bulut bilişim sisteminin birlikte incelendiği kısıtlı sayıda çalışmaya ulaşılmıştır. Bu bağlamda bulut bilişim sisteminin güncel bir teknoloji alanı olması ve kurumsal risk yönetimi ile bağdaştırılması bakımından bu çalışmanın literatüre katkı sağlayacağı düşünülmektedir.

3. BULUT BİLİŞİM SİSTEMİ

Bulut bilişim sistemi; bir işletmenin veya kuruluşun bilgi işlem kaynaklarını ve uygulamalarını herhangi bir konumdan, internet bağlantısı aracılığıyla temin etmesini sağlayan bilgi işlem dağıtımı ve tedarik modelidir. İşletmelerin benimsediği bulut çözüm modeline bağlı olarak; işletmenin donanım, yazılım ve verilerinin tamamı veya bir kısmı kendi teknoloji altyapısında bulunmasına gerek kalmadan diğer kuruluşlarla paylaşılan ve üçüncü taraf şahıslar tarafından yönetilen bir teknoloji merkezinde bulunabilir. Bulut bilişim teknolojisinin de iki önemli kavram yer almaktadır. Bunlar; "Bulut Servis Sağlayıcı-BSS" ve "Çoklu Kiracı" kavramlarıdır. BSS, teslimat, barındırma, izleme ve farklı uygulamaları gerçekleştiren üçüncü taraf bir bilgi sağlayıcısıdır. İşletmeler, bulut çözümlerine bağlı olarak birden çok bulut servis sağlayıcı ile işlemler gerçekleştirebilir. Kiracı ise; bulut bilişimde kaynakları ve teknolojileri paylaşan birçok kiracı arasında yer alan tek bir kiracı demektir (Oscar vd., 2015: 46).

3.1. Bulut Bilişim Sistemi Dağıtım ve Hizmet Modelleri

Ulusal Teknoloji Standartları Enstitüsü (National Institute of Standards of Technology-NIST)'ne göre en yaygın bulut bilişim dağıtım modelleri aşağıdaki gibidir (Mell ve Grance, 2009: 6):

- Özel Bulut: Bulut altyapısı sadece tek bir işletme için işlem gerçekleştirir. Bulut hizmeti işletmenin içinde veya dışında; işletmenin kendisi ya da üçüncü bir şahıs tarafından yönetilir.
- Topluluk Bulutu: Bulut altyapısı birkaç işletme tarafından paylaşılır ve ortak ilgi alanlarına sahip (misyon, sektör iş birliği, uyumluluk gereksinimleri vb.), belirli bir topluluğu destekler. Topluluk bulutu, işletmenin içinde veya dışında; işletmenin kendisi ya da üçüncü bir şahıs tarafından yönetilir.
- Genel Bulut: Bulut altyapısı; genel halk veya büyük bir endüstri grubu tarafından kullanılabilir. Bulut hizmetleri, üçüncü bir şahıs tarafından yönetilir.
- Hibrit Bulut: Bulut altyapısı; hassas ve önemli bilgilerden oluşan, standartlaştırılmış veri ve uygulama taşınabilirliği sağlayan iki veya daha fazla buluttan (özel, topluluk veya genel) oluşur.

Bulut servis sağlayıcı tarafından sunulan bulut çözümleri; genellikle bulut hizmet modelleri olarak adlandırılmaktadır. En yaygın olanları aşağıdaki gibidir (Mell ve Grance, 2009: 7).

- Yazılım Hizmeti (Software as a Service-SaaS): İşletmelerin belirli işlevleri veya süreçleri (e-posta, müşteri yönetimi sistemleri, kurumsal kaynak planlama sistemleri, elektronik tablolar vb.) gerçekleştirmek için kullandığı uygulamalardır.
- Platform Hizmeti (Platform as a Service-PaaS): Sistem geliştirme ortamları kurarak müşterilerine; bulut servis sağlayıcının altyapısında kullanılan uygulama sistemlerinin ve programlarının oluşturulmasını kolaylaştıran sistem araçları sağlamaktadır.
- Altyapı Hizmeti (Infrastructure as a Service-IaaS): Bulut servis sağlayıcı, bütünsel bir sanal veri merkezi kaynağı (ağ, bilgi işlem kaynakları, depolama kaynakları vb.) sağlamaktadır.

3.2. Bulut Bilişim Sisteminin Faydaları ve Riskleri

Bulut bilişim sisteminin sağladığı fırsatlardan ve potansiyel avantajlardan bazıları şunlardır:

Maliyet Tasarrufu: Bulut bilişim sistemini kullanan işletmeler, sürekli olarak kullanmayacağı ekipmanı satın almak veya kiralamak yerine yalnızca kullandıkları bilgi işlem kaynakları için ödeme yapmaktadır. İşletme, teknoloji ihtiyaçlarını karşılamak için bulut bilişim sistemini kullanılıyorsa artık veri aktarımıyla ilişkili fiziksel alan gereksinimlerine ve hizmet maliyetlerine katlanmasına gerek kalmamaktadır (Ryan, 2013: 2264).

Dağıtım Hızı: Bulut hizmeti sağlayıcıları, bilgi işlem kaynaklarına olan ihtiyacı çoğu bilgi teknolojisi işlevinden daha hızlı bir şekilde gerçekleştirebilir. Bilgi işlem ve uygulama taleplerini gerçekleştirme süresi; aylardan haftalara, haftalardan günlere ve günlerden saatlere dönüştürülebilir (Khan vd., 2012:1289).

Teknoloji Kaynaklarının Uyumu ve Ölçeklenebilirliği: Bir işletme işlem kapasitesini, sermaye harcamaları olmadan azaltabilir veya yüzlerce veri sunucusuna yükseltebilir. Bu özellik işletmenin, yüksek talep dönemlerini karşılamak için bilgi işlem kapasitesine yatırım yapmadan, gerektiğinde bilgi işlem faaliyetlerini gerçekleştirmek için büyük miktarda kaynak elde etmesine yardımcı olmaktadır (Xiang vd., 2015: 59).

Teknoloji Yönetiminde Esneklik: Bilgi teknolojisi işlevine sahip olmak ve bu işlevi kullanmak maliyetli ve zaman alıcıdır. Bulut bilişim, bir işletmenin temel amaç ve hedeflerine daha fazla zaman ayırmasına olanak tanımaktadır (Xiang vd., 2015: 60).

Çevresel Faydalar: Her işletme özel veri merkezini bulut bilişim sistemiyle değiştirirse, önemli ölçüde daha az güç tüketimi, karbon emisyonları ve fiziksel alan kullanımı gerçekleşecektir.

COSO'nun kurumsal risk yönetimi entegre çerçevesinde tanımlandığı gibi risk, bir olayın meydana gelme ve hedeflere ulaşılmasını olumsuz yönde etkileme olasılığıdır. Risk türleri (güvenlik, bütünlük, kullanılabilirlik, performans vb.), farklı teknoloji sistemlerinde olduğu gibi bulut bilişim sisteminde de aynıdır. İşletmeler tarafından bulut bilişim çözümleri benimsendiğinde (bulut çözümlerinin nasıl ve hangi amaçla kullanıldığına bağlı olarak) risk seviyesi ve risk profili değişiklik gösterecektir. Bunun nedeni, işlemler için kullanılan bulut servis sağlayıcı ile risk olayları (doğal ve artık risk) arasındaki, olasılık ve etkide meydana gelen artış veya azalışlardır.

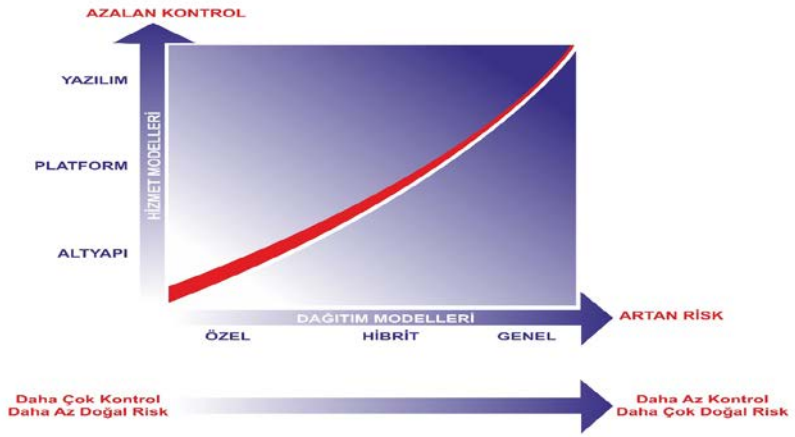
Bulut bilişim sistemi ile ilgili önemli risklerden bazıları ise aşağıdaki gibi sıralanabilir.

- Yıkıcı Güç Olması: Bulut bilişimin, inovasyonu kolaylaştırma ve maliyet tasarrufu sağlama yönleri, bazı işletmeler için risk olarak görülebilir. Piyasaya giriş engellerini azaltarak bazı iş modellerini tehdit edebilir hatta gelecekte tamamen ortadan kaldırabilir (Mansouri, 2016: 929).

- Bulut Sisteminin Diğer Kiracıları ile Aynı Risk Ortamında Olunması: Bir işletme, üçüncü taraflarca yönetilen bulut sistemi çözümlerini benimsediğinde; yasal sorumluluk, risk evreni, olay tanımlama, olay müdahalesi ve diğer alanlar açısından bağımlılık ilişkisi kurmaktadır (COSO, 2012: 4).
- Şeffaflığın Olmaması: Bulut servis sağlayıcının süreçler, operasyonlar, kontroller ve metodolojiler hakkında ayrıntılı bilgi vermesi mümkün değildir. Örneğin, bulut bilişim müşterileri; verilerin depolanma konumları, bilgi işlem kaynaklarını tahsis etmek için kullanılan algoritmalar, özel kontroller ve müşteri verilerinin nasıl kullanıldığına dair çok az bilgiye sahiptir (Ramgovind vd., 2010: 3).
- Güvenilirlik ve Performans Sorunları: Sistem hatası, herhangi bir bilgi işlem ortamında meydana gelebilen ve bulut bilişimde büyük problemler ortaya çıkaran bir risk olayıdır. Bulut sistemini kullanan işletme, bulut sistemi altyapısına beklenmedik bir kaynak talebinde bulunursa bulut servis sağlayıcı çözümleri bazen bu işlemi karşılayamayabilir (Christodorescu vd., 2009: 99).
- Satıcıya Bağımlılık ve Birlikte Çalışma Eksikliği: Bulut servis sağlayıcı, bulut çözümleriyle birlikte yazılım geliştirme araçları da sunmaktadır. Bu araçlar yalnızca bulut servis sağlayıcının özel çözüm yapısında yer alan uygulamalarla kullanılabilirler. Sonuç olarak, bu yeni uygulamalar, bulut çözümünün dışında kalan sistemlerle çok iyi çalışmayabilir (Mansouri, 2016: 931).

- Güvenlik ve Uyumluluk Sorunları: Bulut bilişimde veriler, müşteri işletmenin doğrudan kontrolü dışındaki donanımlarda yer almaktadır. Kullanılan bulut çözümüne (yazılım hizmeti, platform hizmeti, altyapı hizmeti) bağlı olarak, müşteri işletme, ağ işlemlerini veya güvenlik olaylarını günlük olarak takip edemeyebilir (Carlyle vd., 2010: 172).
- Yüksek Etkili Siber Saldırı: Bulut servis sağlayıcı altyapısı ile çalışan birden çok işletmenin birleştirilmesi, siber saldırı olasılığını artırmaktadır. Bu nedenle, çoğu durumda bulut servis sağlayıcı çözümünün doğal risk seviyeleri; gizlilik ve veri bütünlüğü riskleri açısından daha yüksek seviyededir (Carlyle vd., 2010: 173).
- Veri Sızıntısı Riski: Çoklu kiracı ortamında, özel olarak ayrılmış sunucular ve kaynaklar yalnızca bir işletme tarafından kullanıldığında veri sızıntısı riski oluşmaktadır. Bu veri sızıntısı riskinin; veri gizliliği ve gizlilik gereksinimlerinin karşılanması açısından ek bir incelemeye tabi tutulması gerekmektedir (Mulia vd., 2013: 385).
- Bilgi Teknolojileri Organizasyon Değişiklikleri: Bulut bilişim sistemi kapsamlı bir şekilde benimsenirse, işletmelerin altyapı, teknoloji, uygulama ve bakım alanlarında daha az teknolojisi personeline ihtiyacı olacaktır. Bu durum, bilgi teknolojisi personelinin bağlılığını ve motivasyonunu etkilediğinden işletme için risk unsuru oluşturmaktadır (Carlyle vd., 2010: 174).
- Bulut Servis Sağlayıcının Uygulanabilirliği: Bulut servis sağlayıcıları genellikle yeni şirketlerdir. Bu nedenle, bulut bilişim hizmetlerinin tahmini olarak uzun ömürlülüğü ve kârlılığı bilinmemektedir. Bazı bulut servis sağlayıcılarının maliyetlerinin yüksek olması, bulut bilişim hizmetine yönelik talepleri azaltmaktadır (Rasheed, 2014: 366).

Bulut bilişim risklerinden herhangi birinin gerçekleşmesi istenmeyen sonuçlar doğuracağından, bu risklerin dikkatli bir şekilde değerlendirilmesi gerekir. Ayrıca işletmeler bulut bilişim sisteminin, çalışma ortamı üzerindeki risklerini ve diğer etkilerini belirlemeli ve bunları kurumsal risk yönetimi sisteminde değerlendirmelidir (Mulia vd., 2013: 387). Bazı durumlarda işletme yönetimi, bulut servis sağlayıcıların işletmenin operasyonları ve risk profili üzerindeki potansiyel etkisini değerlendirmeyi gerçekleştiremeyebilir (Yao vd., 2013: 97). İşletmelerin bulut bilişim çözümünde (özel bulut hariç), daha az doğrudan kontrole ve dolayısıyla daha yüksek düzeyde doğal riske sahip olduklarını bilmeleri çok önemlidir (Feng vd., 2011: 74).



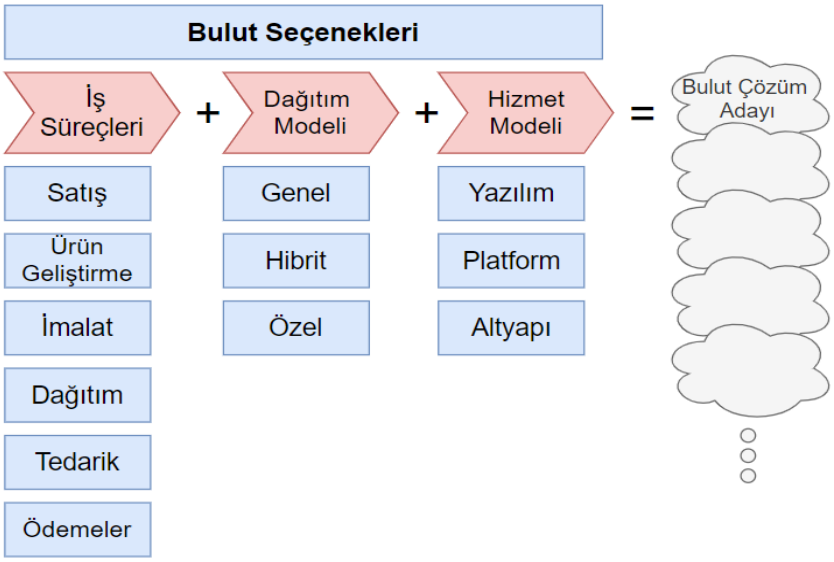
Şekil 1. Bulut Hizmet ve Bulut Dağıtım Modelleriyle Doğal Risk İlişkisi
Kaynak: COSO, 2012: 7.

Şekil 1, bulut bilişim sisteminin hizmet ve dağıtım modellerine bağlı olarak işletmelerin kontrol derecesini göstermektedir. Spesifik olarak işletmeler açısından, maksimum kontrol ve minimum doğal risk derecesi, altyapı hizmeti (dağıtım modeli özel bulut) ile ilişkilidir. Bununla birlikte, yazılım hizmeti (dağıtım modeli genel bulut), en az miktarda kontrolü elinde tutar ve en yüksek düzeyde doğal riski kabul etmektedir. Her durumda işletme yönetimi, bulut bilişim ile ilgili gerekli kontrolleri belirleyeceğinden, bulut dağıtım ve hizmet sağlama modellerini, kabul edilebilir risk seviyeleri bağlamında değerlendirmelidir (Chang vd., 2016: 28).

4. BULUT BİLİŞİM SİSTEMİNDE KURUMSAL RİSK YÖNETİMİ YAKLAŞIMI

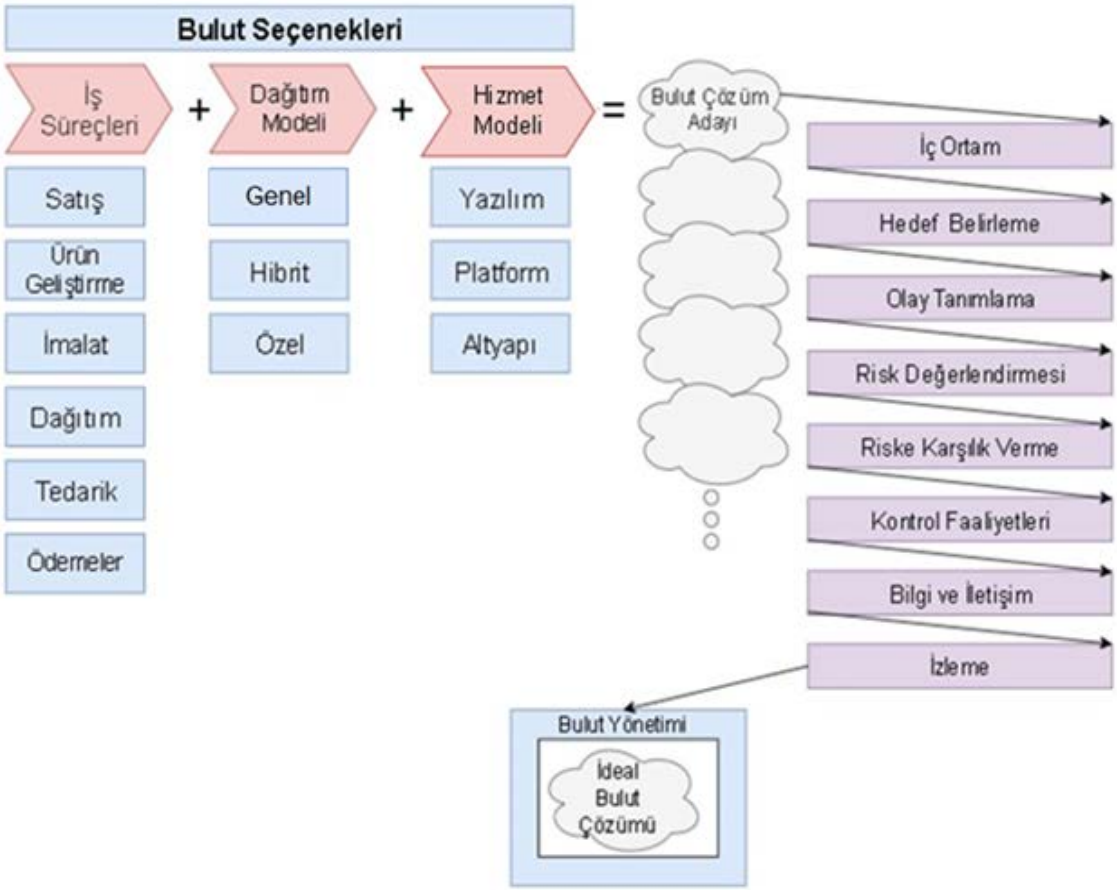
Bulut bilişim sistemi, işletmelerin kurumsal risk yönetimi sürecinde bir faaliyet olarak değerlendirilmelidir. Her bir faaliyette olduğu gibi eylem planlarını önceden tanımlamak işletmelerin başarı şansını artırmaktadır. Dolayısıyla, bulut bilişim sisteminin özelliklerini açıkça tanımlayan iyi bir plan, işletme yönetiminin sağlıklı kararlar almasını kolaylaştıracaktır (Armbrust vd., 2010: 53). Bulut bilişime kurumsal risk yönetimi sisteminin dahil edilmesi için gereken ön koşullar; güçlü bir yönetim modeli, doğru bir raporlama yapısı, dahili bilgi teknolojileri işlemleri ve olayların doğru bir şekilde anlaşılmasını ve tanımlanmasını sağlayan risk iştahından oluşmaktadır (Oscar vd., 2015: 49).

Bazı yöneticiler, risk değerlendirmelerini ve yönetim programlarını isteğe bağlı olarak gerçekleştirmektedir. İşletmelerin detaylı bir risk değerlendirmesi yapmadan, kurumsal risk yönetimi sürecinde bulut bilişim sistemini benimsemeleri olağan kabul edilebilir. Bulut bilişim stratejisi tanımlanırken, işletmelerin yönetim programlarına dahil edilmesi gerekir. Kaliteli ve etkili kurumsal risk yönetimi uygulamalarını kullanmadan bulut bilişim sistemini benimsemiş işletmeler, risk değerlendirmesi yaparak ve bulut bilişim sistemini yönetim programlarına dahil ederek ihtiyatlı adımlar atmış olacaktır (Krutz ve Vines, 2010: 19).



Şekil 2. Bulut Bilişim Sistemi Çözüm Oluşturma
Kaynak: COSO; 2012: 8.

Şekil 2, bulut bilişim destekli iş süreçlerine; dağıtım ve hizmet modelleri arasından çeşitli şekilde seçim yapılarak belirli bir bulut çözümü adayının belirlendiğini göstermektedir. İşletmelerin bulut bilişim paradigmasında, kurumsal risk yönetimi sistemine uyum derecesi; büyük ölçüde bulutun desteklediği iş süreçlerine, dağıtım modeline, hizmet sağlama modeline, bulut servis sağlayıcı risklerine ve kontrol ortamına bağlıdır. Birçok bulut bilişim senaryosunda işletmeler, teknolojilerle ilgili yönetim süreçlerinde tam veya doğrudan kontrole sahip değildir (Mulia vd., 2013: 385). İşletme yönetimi, bulut çözümüyle ilişkili potansiyel olayların risk iştahını belirlemelidir çünkü bu olaylardan bazıları yönetimin kontrolünden çıkarak bulut servis sağlayıcılarını etkileyebilir.



Şekil 3. Kurumsal Risk Yönetiminin Bulut Bilişim Sistemine Uygulanması
Kaynak: COSO, 2012: 9.

Bulut bilişim sisteminin benimsenmesi işletmeler için büyük bir değişiklik yaratabilir. İşletme yönetimi, riskleri etkili bir şekilde değerlendirmek ve yönetmek için kapsamlı ve detaylı kurumsal risk yönetimi çerçevesi kullanmalıdır. COSO'nun kurumsal risk yönetimi entegre çerçevesi, belirli bir bulut çözüm adayını oluşturmak ve bulut bilişim yönetim programını geliştirmek için ortak bir dil ve temel oluşturmaktadır. COSO kurumsal risk yönetimi çerçevesi, orijinalde bir küp olarak gösterilmektedir. Ancak Şekil 3'te COSO kurumsal risk yönetimi entegre çerçevesi, belirli bir bulut çözüm adayının işletmeye getireceği avantajları ve dezavantajları anlamak için bulut çözüm adayının her bir kurumsal risk yönetimi bileşenine (iç ortam bileşeninden başlanarak sırasıyla izleme bileşenine kadar) uygulandığı bir yol olarak gösterilmektedir. Her bir bulut çözümü adayı için süreç

tamamlandığında ideal bulut çözümü; bulut yönetimini kurmak ve sürdürmek için gerekli şartlarla birlikte ortaya çıkacaktır (Mell ve Grance, 2009: 5). COSO kurumsal risk yönetimi çerçevesi, bulut çözümünün uygulandığı durumlarda, bulut programının tüm ana yönlerini (hedefler, risk değerlendirme, risk tepkisi vb.) yönetimin gereksinimlerine göre ele almaktadır.

Etkili bir bulut programı, bulut çözümünün belirlenmesinin ardından COSO kurumsal risk yönetimi çerçevesiyle birlikte kullanılmasıyla elde edilebilir (COSO, 2012: 9). İşletme yönetimi, COSO kurumsal risk yönetimi bileşenleri bağlamında bulut çözümü adaylarını değerlendirerek, her bir bulut çözümü senaryosuyla ilgili riskleri ve kabul edilebilir veya azaltılabilir risk stratejilerini özlü bir şekilde belirleyebilmektedir. Bu değerlendirme işletme yönetiminin, ideal bulut çözümü seçeneklerini belirlerken ve iyi planlanmış bir bulut yönetim programını oluştururken doğru ve ihtiyatlı kararlar almasını sağlayacaktır. Kurumsal risk yönetimi bileşenlerinin bulut bilişim sistemine yönelik açıklamaları aşağıdaki gibidir (COSO, 2012: 10):

- İç Ortam: İç ortam bileşeni, risklerin ve kontrollerin nasıl değerlendirildiği açısından işletmelerin risk iştahının temelini oluşturur ve tanımlamalar yapar. Örneğin, işletme yönetiminin riskten kaçınma kültürü varsa, bu politika bulut dağıtımı ve hizmet modelleri için uygulanabilirliği sınırlayacaktır. Bu durum için özel bulut çözümleri, kabul edilebilir alternatif olarak değerlendirilecektir.
- Hedef Belirleme: İşletme yönetimi, bulut bilişim sisteminin işletme hedefleriyle ne derece uyumlu olduğunu değerlendirmektedir. Koşullara bağlı olarak bulut bilişim, işletmenin mevcut hedeflere ulaşma olasılığını artıracak veya yeni hedeflerin belirlenmesini sağlayacak rekabet avantajı sunabilir.
- Olay Tanımlama: İşletme yönetimi, hedeflere ulaşılmasını etkileyebilecek olayları belirlemekten sorumludur. Bir işletmede olay tanımlama ve risk değerlendirme süreçlerinin karmaşıklığı, bulut servis sağlayıcılarıyla birlikte artış gösterebilir. İşletme yönetimi risk olaylarını belirlerken ve değerlendirirken dış faktörleri (düzenleyici, ekonomik, doğal, politik, sosyal ve teknolojik) ve işletmenin iç faktörlerini (kültür, personel ve finansal durum) dikkate almalıdır.
- Risk Değerlendirmesi: İşletme yönetimi, her bir bulut çözüm seçeneği ile ilişkili risklerin potansiyel etkisini belirlemek için bulut stratejisiyle bağlantılı risk olaylarını değerlendirmelidir. İşletmelerde bulut çözümüne geçmeden önce risk değerlendirmesi tamamlanmalıdır. Bulut bilişim, risk değerlendirmesinin aşağıdaki kritik noktalarını etkileyebilir:

  Risk Profili: Bir işletmenin risk profili, yönetmesi gereken risklerin tamamını kapsamaktadır. Risk olasılığındaki değişiklikler, risklerin potansiyel etkisi ve bulut servis sağlayıcısının risk evrenine dahil edilmesi bir kuruluşun risk profilini değiştirmektedir.

  Doğal (İçsel) ve Kalıntı (Artık) Risk: Bir işletme, olayların doğasında var olan riskleri değerlendirdikten sonra risk yanıtları geliştirmeli ve artık riskleri belirlemelidir.

  Olasılık ve Etki: İşletme tarafından bulut çözümleri gerçekleştirildiğinde, birçok durumda belirli olayların olasılığı ve etkisi değişir. Bu olayların olasılığını ve etkisini doğru bir şekilde belirleyebilme; işletmenin kapsamlı, doğru ve güncel bir risk envanterine sahip olmasına bağlıdır.

- Riske Karşılık Verme: Bulut bilişimle ilgili organizasyonel hedefler bağlamında riskler tanımlandıktan ve değerlendirildikten sonra, işletme yönetiminin risk tepkisini belirlemesi gerekir. Riske karşılık verme süreci dörde ayrılmaktadır. Bunlar:

  Kaçınma: Riske neden olan faaliyetlerden uzak durmaktır (bulut bilişime geçmemek veya yalnızca özel bulut çözüm türlerini uygulanabilir seçenekler arasında değerlendirmek).

  Azaltma: Risk olasılığını, risk etkisini veya her ikisini de azaltmak için kontrol faaliyetlerinin uygulanması ve önlemlerin alınmasıdır.

  Paylaşma: Riskin bir kısmını aktararak veya paylaşarak (örneğin sigorta yaptırılması) risk olasılığını veya risk etkisini düşürmektir.

  Kabul: Risk olasılığı veya etkisi üzerine hiçbir önlem almamaktır. İşletmeler, hibrit veya genel bulut çözümünde, üçüncü taraflara bağlı oldukları için riskleri doğrudan azaltma imkânları kısıtlanmaktadır.

- Kontrol Faaliyetleri: Geleneksel kontrol türleri bulut bilişim sistemi için de geçerlidir. Bulut bilişim sisteminin getirdiği fark, kontrol sorumluluklarının bazılarının işletmeye, bazılarının da bulut servis sağlayıcısına bırakılmasıdır. Kontrol faaliyetleri yeterli seviyede olmayan bir işletmenin, bulut çözümünü kullanması iç kontrol faaliyetlerini olumsuz yönde etkileyebilir.

- Bilgi ve İletişim: İşletme yönetiminin, faaliyetleri etkin bir şekilde yürütmek ve ilgili riskleri analiz etmek için, çeşitli kaynaklardan zamanında ve doğru bir şekilde bilgi temin etmesi ve iletişim kurması gerekir. Ayrıca, işletme yönetiminin bilgi ve iletişim gereksinimlerinin karşılanması, ek veya farklı bilgi süreçlerini de gerektirebilir.

- İzleme: Risk karşılıklarının sonuç vermemesi, kontrol faaliyetlerinin etkisiz olması ve kurum hedeflerinin değişmesi bulut bilişim sistemini etkilemektedir. İşletme yönetimi, bulut programının ilgili riskleri yeterince ele aldığını ve işletmenin hedeflerine ulaşmayı kolaylaştırdığını doğrulamak için kurumsal risk yönetimi programının etkinliğini izlemelidir. Bilgi işlem ortamından genel veya hibrit bulut çözümünü kullanan bir işletme, kurumsal risk yönetimini; bulut servis sağlayıcı ve kurumsal risk yönetimi bileşenlerinden oluşan bir kombinasyona dönüştürmektedir. Şekil 4'te, bu kombinasyon gösterilmektedir.

Şekil 4. Kurumsal Risk Yönetimi Bileşenleri Evreni ile Bulut Servis Sağlayıcının Birleştirilmesi
Kaynak: COSO, 2012: 12.

İşletmelerin verileri, diğer bulut kiracılarıyla paylaşılan bir ortamda tutulmaktadır. Bulut servis sağlayıcısının ve diğer kiracıların davranışları, organizasyon üzerinde doğrudan bir etkiye sahiptir. Bulut servis sağlayıcısının maruz kaldığı riskler, bulut müşterilerini etkileyebileceği için bu risklerin bulut çözümünü kullanan işletmelerin risk profiline dahil edilmesi gerekir. İşlem ortamlarının bu şekilde harmanlanması, organizasyonun risk profilini değiştirebilir ve yeni kontroller gerektirebilir (Krutz ve Vines, 2010: 23). Bulut bilişimde, risk değerlendirme sürecinin bir parçası olarak işletme yönetiminin, diğer bulut kiracısı olan işletmelerin risk bilgilerini de (kimlikleri, kullandıkları uygulamalar, siber saldırıların hedefi olma olasılıkları vb.) dikkate alması gerekebilir. İşletme yönetimin kurumsal risk yönetimi programı, bulut servis sağlayıcısı ve kurumsal risk yönetimi bileşenlerini birlikte ele almalıdır. İşletme yönetimi; kurumunu, bulut servis sağlayıcısını ve diğer bulut kiracılarını etkileyebilecek riskleri ve olayları belirlemelidir.

5. KURUMSAL RİSK YÖNETİMİNDE BULUT BİLİŞİM SİSTEMİ İÇİN RİSK KARŞILIKLARI

Bulut bilişim sistemi ve farklı teknoloji uygulamalarının ortaya çıkmasıyla birlikte işletmeler, hızla değişen bir teknoloji ortamında faaliyet göstermeye başlamışlardır. İşletme yönetimlerinin, kurumsal risk yönetimi süreçlerini bu değişen ortama göre uyarlamaları kaçınılmaz bir durum olmuştur. Aşağıda bulut bilişim sistemi ile ilgili önemli risklerden bazıları için önerilen risk karşılıkları açıklanmaktadır (COSO, 2012: 13):

1. İzinsiz Bulut Bilişim Kullanımı Riskine Verilen Karşılık

İşletmeler, bulut hizmetlerinin izinsiz kullanımını önlemek ve tespit etmek için kontrol faaliyetleri gerçekleştirmelidir. İzinsiz kullanılan bulut bilişim için işletmelere önerilen bazı risk karşılıkları aşağıdaki gibidir (COSO, 2012: 13);

- İşletme yönetiminin uygun gördüğü iş süreçlerinin ve verilerinin, bulut bilişim sistemine göre oluşturulması,
- Bulut bilişim hizmetlerini kullanma sürecinde işletme içerisinden kimin yetkili olduğunun belirlenmesi,
- Yetkili bulut servis sağlayıcısının belirlenmesi ve
- Bulut servis sağlayıcısı ile ilişkilerin yönetimi konusunda, politikaların ve iletişim stratejilerinin tanımlanması..

2. Şeffaflık Eksikliği Riskine Verilen Karşılık

İşletmeler tarafından kullanılan bilgilerin eksik, hatalı ya da yanlış olması durumunda, bulut servis sağlayıcısının risk değerlendirmesini yapmak doğru olmayabilir. Bulut servis sağlayıcının operasyonları ve kontrollerine ilişkin fikir edinme zorluklarının üstesinden gelmek için işletme yönetimi, yapılan sözleşmeden başlayarak gerçekleştirilen işlemlere kadar sorgulamalar yapmalıdır. Ayrıca işletme yönetimi, her bir bulut servis sağlayıcı ile yapılan sözleşmeye denetim hakkı maddesi eklemeye çalışmalıdır. İşletme yönetimi (tercihen bulut servis sağlayıcı faaliyetine başlamadan önce) bulut servis sağlayıcının risk olaylarını nasıl ele alacağını belirlemek için görüşmeler yapmalıdır. İşletme yönetimi; bulut servis sağlayıcının

kontrol ortamı ve kalitesi hakkında daha fazla bilgi almak için iç denetim fonksiyonunun bir değerlendirme yapmasını sağlayabilir (Shi vd., 2010: 1).

3. Güvenlik, Uyumluluk, Veri Sızıntısı ve Veri Yetkisi Risklerine Verilen Karşılık

İşletme faaliyetlerinin yürürlükteki yasa ve yönetmeliklere uygun olarak sürdürülmesi zorunluluğu, veri depolama ve veri işleme kontrol yapılarının mevcut durumunun incelenmesini gerektirmektedir. Sözleşmede, bulut servis sağlayıcının işletme adına uygunluk ve yasal gerekliliklerin karşılanmasına ilişkin sorumlulukları açıkça belirtilmelidir. Ülke konumuna (yerel veya uluslararası) ilişkin müşteri verileri, sözleşme şartlarında belirlenmeli ve veri koruma yasasına uygunluğu açısından değerlendirilmelidir. Bulut çözümüne geçmeden önce işletme yönetiminin, işletme verileriyle ilgili yasal sorumluluklarını bilmesi çok önemlidir. Örneğin, Almanya'daki verileri kontrol eden Amerika Birleşik Devletleri merkezli bir bulut servis sağlayıcıyı ele alırsak; bu bulut servis sağlayıcı, Almanya veri koruma yasalarına ve Avrupa Birliği veri koruma ve bildirim yasalarına uygun olmalıdır. Ayrıca bulut çözümünde uyumluluk ve veri yetkisi, işletmelerin yükümlülükleri açısından bakıldığında tüm işlemleri gözden geçirme ihtiyacını artırmaktadır (Ryan, 2013: 2265).

İşletmeler, genel veya hibrit bulut modelini kullanırken verilerinin tam olarak nerede depolandığını kontrol edemezken, bilgilerin içeriğini kontrol edebilir. Risk yönetimi perspektifinden bakıldığında, genel veya hibrit bulut çözümlerini kullanan işletmelerin etkin olarak, veri sınıflandırma politikalarına ve süreçlerine sahip olması kritik öneme sahiptir. Veri sınıflandırma politikaları; hassas kabul edilen ve işletmenin doğrudan kontrolü dışında kullanılması yasaklanmış bilgi türlerini kapsamalıdır. Ayrıca kurumsal veri türlerinin amacına ve önemine yönelik, açıkça iletilmesi ve anlaşılması sağlanmalıdır. Veri sınıflandırma politikaları (COSO, 2012: 14);

- Yasal, düzenleyici, fikri mülkiyet ve güvenlik gereksinimlerini eşleştirmek,
- Çeşitli veri türlerinin hassasiyetini (genel, kısıtlı veya oldukça hassas) belirlemek,
- Veri aktarımı için şifreleme yapmak ve
- Veri erişiminin kimlere verileceğine karar vermek için uygun bilgi ve yetkiye sahip kişileri belirlemek gibi süreçlerle desteklenmelidir.

4. Şeffaflık ve Doğrudan Kontrolden Vazgeçme Risklerine Verilen Karşılık

İşletme yönetimi, iç kontrol ortamının tüm yönlerine doğrudan müdahalede bulunabilir (Baxter vd., 2013: 1271). Genel veya hibrit bulut modellerinde işletme yönetimi, kısmi veya tam olarak kontrolü bulut servis sağlayıcıya aktarmaktadır. Bulut servis sağlayıcı, müşterilerinin kontrol gereksinimlerini makro bir bakış açısıyla sürdürdüğü için müşterileri ihtiyaçlarının tamamını karşılaması pek mümkün değildir. Bulut servis sağlayıcı tarafından sağlanan bulut çözümünü ayrıntılı olarak değerlendirmek ve bulut çözümüne ek kontroller uygulamak işletme yönetiminin sorumluluğudur. İşletme yönetiminin, bulut servis sağlayıcının inisiyatifine vereceği kontroller hakkında iyi bir değerlendirme yapması gerekir. Halka açık bir işletme, finansal tablo beyanlarını etkileyen kontrolleri bulut servis sağlayıcıya vermesi durumunda ilave önlemler uygulamalıdır. Bulut bilişime geçiş, işletme yönetiminin ek bir işlem ya da uygulama yapmayacağı anlamına gelmemektedir (Shi vd., 2010: 1).

Bulut çözümünün kontrol ortamını korumak, işletme yönetiminin ve anlaştığı bulut servis sağlayıcının ortak sorumluluğundadır. Bazı durumlarda, bulut servis sağlayıcı kendi sorumluluklarından birkaçını başka bir bulut servis sağlayıcısına (taşeron) devredebilir, bu da karmaşıklık oluşmasına sebep olmaktadır. Bu tür karmaşık bir durumun gerçekleşmesini önlemek için, bulut servis sağlayıcı sözleşmesi her türlü alt yükleniciyi engellemelidir (Shi vd., 2010: 2). Hibrit veya genel bulut çözümleri kullanan işletmeler, bu çözümlerin kurumun risk iştahıyla uyumlu olup olmadığını belirlemek için bulut servis sağlayıcının kontrol faaliyetlerini değerlendirmelidir. Ayrıca işletmeler, bulut servis sağlayıcı tarafından sürdürülen kontrollerin etkinliğini periyodik olarak incelemelidir. Seçilen bulut hizmeti modeline bağlı olarak işletmeler ve anlaşılan bulut servis sağlayıcı arasındaki kontrol sorumluluğu; uygulama, teknoloji operasyonları ve erişim yönetimi alanlarında paylaşılabilir.

5. Güvenilirlik, Performans ve Yüksek Etkili Siber Saldırı Risklerine Verilen Karşılık

İşletmelerin, sistem hatası ve veri hırsızlığı olaylarına yönelik müdahale prosedürlerinde, bulut servis sağlayıcının bu olaylara nasıl karşılık verdiği de değerlendirilmelidir. Bulut servis sağlayıcının sistem hatası veya güvenlik ihlali, birden fazla kiracıyı etkilemektedir. Bu tür olaylar meydana geldiğinde bulut servis sağlayıcının, her bir kiracının sorunlarını ayrı ayrı ele alma olasılığı düşüktür. İşletme yönetiminin bulut servis sağlayıcıya yönelik müdahale planı, gerçekleşebilecek en kötü senaryoya göre hazırlanmalıdır. Aşağıdaki örnekler, bulut çözümünde sistem arızasına ve siber saldırılara yönelik doğal riskleri ve bu riskleri azaltacak kontrolleri açıklamaktadır (COSO, 2012: 15):

- Sistem Arızası: Herhangi bir bilgi işlem ortamında meydana gelebilecek risk olayıdır. Büyük bir sistem arızasıyla birlikte aynı anda desteğe ihtiyaç duyan birden çok kiracı olması durumunda, öncelik seviyesi düşük işletmeler bulut servis sağlayıcıdan etkin bir hizmet alamayabilir. Sistem arızası riskini azaltabilecek kontroller;
  - İşletme verilerinin kopyalarını saklamak,
  - Bulut çözümü için başka bir hizmet sağlayıcının destek araçlarını kullanmak,
  - Sistem kullanılabilirliğini izlemek için süreçler geliştirmek ve
  - Sistem arızaları esnasında yeterli seviyede destek almak için bu durumu sözleşmede belirtmek şeklinde sıralanabilir.
- Siber Saldırılar: İşletmeler, sistemlerine yönelik her zaman doğal bir siber saldırı riski taşımaktadır. Birden fazla büyük işletmenin bulut servis sağlayıcı altyapısında birleştirilmesi, bilgisayar korsanlarına daha büyük ve daha iyi bir hedef sunmaktadır. Küçük ve büyük bir işletme, bulut servis sağlayıcının altyapısını paylaştığı durumda; küçük işletmenin siber saldırıya uğrama olasılığı, büyük işletmenin olasılığı ile aynı seviyeye gelmektedir. Siber saldırı riskini azaltabilecek kontroller;
  - Bulut servis sağlayıcı çözümlerinde önemli olmayan verileri barındırmak,
  - Bulut çözümlerinde kullanılan veriler üzerinde şifreleme yapmak ve
  - Başka bir bulut servis sağlayıcının çözümünden yararlanmak için işlem devretme stratejisine sahip olmak şeklinde sıralanabilir.

Örneğin, çok iyi bilinen bir bulut servis sağlayıcı (Amazon veya Google), siber saldırı nedeniyle hizmet kesintisi veya güvenlik ihlali yaşarsa, bu durum hızlı bir şekilde duyulacaktır. Bulut servis sağlayıcı; sorunun nedeni, tahmini kurtarma süresi veya olayın etkisi hakkında yeterli açıklama ve çözümleme yapana kadar bulut servis sağlayıcının müşterisi olan işletmeler bu olaydan etkilenmeseler bile itibar olarak zarar görecektir.

6. Yönetmeliklere Uymama Riskine Verilen Karşılık

İşletme yönetiminin, bulut servis sağlayıcı operasyonlarını etkileyebilecek dış ortamdaki değişiklikleri izlemesi gerekir. Düzenlemeler veya telekomünikasyondaki değişiklikler, bulut bilişim üzerinde önemli bir etkiye sahiptir. Sürekli olarak veri gizliliği alanında önemli yasal değişiklikler beklenmektedir. Çeşitli ülkeler, vatandaşlarının kişisel olarak tanımlanabilir bilgilerinin ülke sınırları dışına taşınmasını ve saklanmasını azaltmak için koruyucu önlemler almaktadır. Verileri, bulut servis sağlayıcısına bağlı olarak farklı ülkelerde depolamak yerine, müşteri işletmenin bulunduğu ülke sınırları içinde depolamak gerekir (Armbrust vd., 2010: 55).

7. Satıcıya Bağlı Kalma Riskine Verilen Karşılık

İşletmeler, bulut çözümünü ne kadar çok kullanırsa ve bulut servis sağlayıcısının işlemlerini desteklemek için ne kadar çok katkıda bulunursa, bulut servis sağlayıcısına o kadar bağlı kalır. Hiçbir şey sonsuza dek sürmediği için işletme yönetiminin bulut servis sağlayıcısını değiştirme veya bulut çözümünü bırakma durumunu önceden değerlendirmesi faydalı olacaktır (Feng vd., 2011: 76). Ayrıca işletme yönetimi ek olarak acil durum planı geliştirmelidir.

8. Gerekli Açıklamaları Yapmama Riskine Verilen Karşılık

Kritik iş süreçlerini desteklemek için bulut servis sağlayıcısını kullanan halka açık şirketler, bulut bilişime yönelik yeni bilgi ve açıklamalara ihtiyaç duyabilir. Bulut bilişim çözümlerinin, iş süreçleri ve risk faktörleri üzerindeki potansiyel etkisi bağlamında, düzenleyici kamu kurumlarının; yasal uyumluluk ve şeffaflık ilkelerine göre yaptıkları açıklamaları bu süreçleri gözeterek gerçekleştirmesi gerekir (Shi vd., 2010: 2).

9. Üst Yönetimin Alması Gereken Sorumluluklar

Kurumsal risk yönetimi sürecinde bulut bilişim sisteminin faaliyetlerini etkin bir şekilde yönetmek ve oluşabilecek risklere karşılık verebilmek için üst yönetimin sorumluluklar alması gerekir. Aşağıda üst yönetimin alması gereken temel bulut sorumlulukları belirtilmektedir (COSO, 2012: 21):

- Yönetim Kurulu
  - Bulut bilişim eğilimlerinin farkında olmak,
  - Bulut bilişimin sektöre ve işletmenin iş modeline etkisini tespit etmek,
  - Bulut bilişim hizmetleri gibi bilgi teknolojileri projelerinin farkında olmak ve gözetim altında tutmak,
  - İş ve teknoloji stratejisi bağlamında bulut bilişimin avantajlarını ve risklerini belirlemek,
  - Bulut bilişimin, işletmenin risk iştahı ve kontrol faaliyetleriyle uyumlu olmasını sağlamak için iç denetim kaynaklarından yararlanmak,

- Yönetim Kurulu Başkanı
  - Kuruluşun dış kaynak kullanımına ilişkin bakış açısını ve politikalarını tanımlamak,
  - Bulut bilişimin, işletmenin faaliyetlerini sürdürdüğü sektör üzerindeki etkisini anlamak,
  - İşletmenin bulut bilişimi nerede ve nasıl kullanacağını belirlemek,
- Finansal İşler Müdürü
  - Finansal raporlamada bulut bilişimin kullanımına ilişkin düzenlemeler yapmak,
  - Bulut bilişim ile toplam maliyetleri ve yatırım getirisini değerlendirmek ve izlemek,
  - Bulut bilişimin vergi ve muhasebe işlemlerine yönelik avantajlarını tespit etmek,
  - Bulut bilişim hizmetlerinin gerçekleştirilme sürecinde politikalar ve kontroller uygulamak,
  - Bulut servis sağlayıcıların mali durumunu değerlendirmek,
- Hukuk İşleri Müdürü
  - İşletmede kullanılan bulut bilişim sisteminin yasalara ve düzenlemelere uygun olmasını sağlamak,
  - Bulut çözümünü veya bulut servis sağlayıcısını etkileyebilecek yeni yasaları ve düzenlemeleri takip ederek planlama yapmak,
  - Veri sınıflandırma süreçleri hakkında değerlendirme yapmak,
  - Bulut servis sağlayıcı sözleşmelerini gözden geçirerek kuruluşun çıkarlarını ve haklarını korumak,
  - Farklı ülkelerde yer alan bulut hizmetlerinin kullanılmasıyla ilgili olarak işletme faaliyetlerinin yasal yargı alanı belirlemek,
- Bilişim Kurulu Başkanı
  - Bulut bilişimin mevcut iş stratejilerini ve yeni iş fırsatlarını destekleme potansiyelini tespit etmek,
  - Bulut çözümlerinden yararlanmak ve etkinliğini artırmak için genel bir strateji oluşturmak,
  - Bulut çözümlerinin işletmeye ve mevcut bilgi teknolojisi altyapısına entegrasyonunu kolaylaştırmak,
  - İşletmenin kurumsal risk yönetimi sistemine bulut bilişimin dahil edilmesine yardımcı olmak,
  - Verilerin kullanıcıları da dahil olmak üzere bir veri sınıflandırma şeması oluşturmak,
  - Kaynak sağlama, kullanıcı erişim yönetimi ve kullanıcı değişikliği için bulut süreçleri oluşturmak,
  - Bulut servis sağlayıcı sözleşmelerini belirlemek ve uygulamak,

- Bulut servis sağlayıcı ve diğer bulut kiracı müşterilerin faaliyetlerini takip etmek,

• İç Denetim Müdürü
  - Kontrollerin ve süreçlerin bulut servis sağlayıcı ile paylaşıldığı karma kontrol ortamının tasarımını ve etkinliğini değerlendirmek için periyodik denetimler gerçekleştirmek,
  - Bulut servis sağlayıcı kontrollerinin etkinliğini doğrulamak için bulut servis sağlayıcısını denetlemek,
  - Veri sınıflandırma politikalarına uygunluğu doğrulamak için bulutlarda bulunan verilerin periyodik olarak denetimlerini gerçekleştirmek,
  - Bulut servis sağlayıcısının maliyetlerini ve bu maliyetlerin sözleşmeye uygunluğunu denetlemek,
  - Bulut bilişimin yönetimini değerlendirmek,

Üst düzey yöneticiler tarafından yukarıda değinilen sorumlulukların özverili bir şekilde yerine getirilmesi, bulut bilişim sisteminin uygulanma sürecinde verimliliğin ve etkinliğin artmasına yardımcı olacaktırlar.

6. SONUÇ

Bazı iş çevreleri, internetin 20. Yüzyılın son on yılında yaptığı etki kadar bulut bilişim sisteminin de işletmelerde farklılık yaratarak aynı etkiyi göstereceğini düşünmektedir. Bulut bilişim sistemi, ilerleyen yıllarda teknoloji evriminin tarihsel zaman çizelgesinde izini bırakacaktır. Bulut bilişim sisteminin benimsenmesi ve kabul edilmesi, son on yılın diğer önemli eğilimlerinin (sosyal ağ siteleri, sanal perakendecilik vb.) popülaritesi ve kullanımı ile bağlantılıdır. Bu bağlantı ortamında insanların ve tesislerin görülmemesine rağmen bilişim sistemlerine; iletişimi kolaylaştırması, bilgileri depolaması ve işlerin hızlı bir şekilde yapılmasını sağlaması bakımından büyük ölçüde güvenilmektedir.

15 yıl öncesine kadar merkezi işlem birimleri, bilgisayarları işletmenin görsel vitrinini oluşturacak şekilde konumlandırmakta ve üst düzey yöneticiler bu birimleri kontrol ederken fiziksel güvenlik önlemlerini, veri merkezlerinin büyüklüğünü ve kullanılan ekipman miktarını belirterek kendilerine prestij sağlamaktaydılar. O dönemin üst düzey yöneticileri, işletme bilgi varlıklarının, kolayca doğrulanabilen ve iyi korunan veri depolarında saklandığından kuşku duymuyorlardı. Günümüzde mevcut bulut bilişim teknolojisiyle birlikte geçmiş ve yeni nesil üst düzey yöneticiler, merkezi işlem birimlerini gezmeden ve işletmenin bilgi varlıklarının tam konumu hakkında detaylı bilgi sahibi olmadan çok daha ucuz bir teknoloji kullanma fırsatı yakalamaktadır.

Bulut bilişimin kendine özgü yönleri, kurumsal risk yönetimi programları için yeni zorluklar oluşturabilir. Bulut bilişim sisteminin benimsenmesi, mevcut ya da tahmin edilen riskler gerçekleştiğinde işletme ve işletme yönetiminin ne kadar etkileneceğine odaklanmaktadır. Bulut bilişim sisteminin, işletmelerin başına gelebilecek olumsuz olaylardan (suç eylemleri, insan hatası, öngörülemeyen kazalar ve kesintiler vb.) kesin olarak kaçınmasını sağlayacağı yönündeki düşünce doğru değildir. Bulut bilişim programının

etkinliği; risklere karşılık verme stratejileriyle birlikte gerçekleşmesi muhtemel risklerin doğru bir şekilde analiz edilmesine bağlıdır. Böylece işletme yönetimi, COSO kurumsal risk yönetimi çerçevesinden yararlanarak, her bir bulut çözümünün gerektirdiği riskler ve risk yanıtları evrenini belirlemede etkili ve tutarlı bir yaklaşıma sahip olacaktır.

Bulut bilişim sistemi, COSO kurumsal risk yönetimi çerçevesi paralelinde gerekli önlem ve kontrollere uygun olarak kullanıldığında işletmelere teknoloji odaklı kurumsal risk yönetimi sürecinde; maliyet, işlem takibi, verimlilik, işlem hızı, kaynak kullanımı, bilgi kapasitesi, sürdürebilirlik ve bilgi paylaşımı gibi çok sayıda alanda avantaj sağlayabilir. Üst düzey yöneticiler, bulut bilişim ile ilgili risklerin ve diğer sorunların farkında olarak, muhtemelen geleceğin en popüler bilgi işlem modeli haline gelecek olan bu dinamik ve gelişen ortamda risklerini yönetirken, işletmelerinin hedeflerine ulaşma olasılıklarını artıracaklardır. Bulut bilişim sisteminin güncel bir teknoloji alanı olması ve kurumsal risk yönetimi ile bağdaştırılması bakımından literatüre katkı sağlayacağı düşünülmektedir. Bu çalışmanın, benzer ya da daha kapsamlı çalışmalara örnek teşkil ederek farklı alanlarda da kullanılabileceği öngörülmektedir.

KAYNAKLAR

Abdelrafe, E. – Burairah, H. – Samy, A. – Khalid, K. – Mohamed, D. – Selamat, A. – Rashed, A. (2016), "A New Conceptual Framework Modelling for Cloud Computing Risk Management in Banking Organizations", International Journal of Grid and Distributed Computing, 9(9), pp. 137-154.

Ali, M. - Khan, S.U. - Vasilakos, A. V. (2015), "Security in Cloud Computing: Opportunities and Challenges', Information Sciences, 305(3), pp. 357-383.

Akbaba, A. (2019), "Bulut Muhasebe ve İşletmelerde Uygulanması", Muhasebe ve Finansman Dergisi, 82(21), ss. 21-40.

Armbrust, M. - Fox, A. - Griffith, R. - Joseph, A. D. - Katz, R. - Konwinski, A. - Lee, G. - Patterson, D. - Rabkin, A. - Stoica, I. - Zaharia, M. (2010), "A View of Cloud Computing", ACM Communications, 53, pp. 50–58.

Baxter, R. - Bedard, J. - Hoitash, R. - Yezegel, A. (2013), "Enterprise Risk Management Program Quality: Determinants, Value Relevance, and The Financial Crisis", Contemporary Accounting Research, 30(4), pp. 1264–1295.

Carlyle, A. G. - Harrell, S. L. - Smith, P. M. (2010), "Cost-effective HPC: The Community or The Cloud?", Cloud Computing technology and science, IEEE Second International Conference, pp. 169-176.

Ciğer, A. - Kınay, B. (2018), "Bağımsız Denetim Firmalarının Bulut Bilişim Uygulamalarını Benimseme Düzeylerine Yönelik Nitel Bir Araştırma: Antalya İli Örneği", Muhasebe Bilim Dünyası Dergisi, 20(3), ss. 629-649.

Chang, V. - Kuo, Y. H. - Ramachandran, M. (2016), "Cloud Computing Adoption Framework: A Security Framework for Business Clouds", Future Generation Computer Systems, 57(1), pp. 24-41.

Christodorescu, M. - Sailer, R. - Schales, D. L. – Sgandurra, D. – Zamboni, D. (2009), "Cloud Security is not (just) Virtualization Security: A Short Chapter", Proceedings of the 2009 ACM Workshop on Cloud Computing Security, pp. 97-102.

Coso, (2012), "Enterprise Risk Management for Cloud Computing", Committee of Sponsoring Organizations of The Treadway Commission (COSO), New York.

Desender, K. A. (2007) "On The Determinants of Enterprise Risk Management Implementation", SSRN Electronic Journal, pp. 1-26.

Erdem, B. (2020), "Bulut Bilişim Uygulama Maliyetlerinin, Müşteri İşletmeler Tarafından Muhasebeleştirilmesi", Muhasebe ve Denetime Bakış, ss. 233-252.

Feng, D. G. - Zhang, M. - Zhang, Y. (2011), "Study on Cloud Computing Security", Journal of Software, 22(1), pp. 71-83.

Grace, M. F. - Leverty J. T. - Phillips, R. D. - Shimpi, P. (2015), "The Value of Investing in Enterprise Risk Management", The Journal of Risk and Insurence, 82(2), pp. 289-316.

Khan, A. - Yan, X. - Tao, S. - Anerousis, N. (2012), "Workload Characterization and Prediction in The Cloud: A Multiple Time Series Approach", Network Operations and Management Symposium (NOMS), pp. 1287-1294.

Krutz, R. L. - Vines, R. D. (2010), Cloud Security: A Comprehensive Guide to Secure Cloud Computing, Indianapolis: Wiley Publishing.

Malik, M. - Zaman, M. - Buckby, S. (2020), "Enterprise Risk Management and Firm Performance: Role of the Risk Committee", Journal of Contemporary Accounting and Economics, 16, pp. 1-20.

Mansour, N. (2016), "Adaptive Data Replication Strategy in Cloud Computing for Performance Improvement", Frontiers of Computer Science, 10(5), pp. 925-935.

Marsh, M. "Kurumsal Risk Yönetimi: Risk Yönetiminde Daha Stratejik Yaklaşım Arayışları", Http://www.Marsh.Com.Tr/Documents/Press_Release_ERM.Pdf, (23/04/2021).

Mell, P. - Grance, T. "The NIST Definition of Cloud Computing", http://csrc.nist.gov/publications/PubsSPs.html#800-145, (13.08.2021).

Mulia, W. D. - Sehgal, N. - Sohoni, S. - Acken, J. M. - Stanberry, C. L. - Fritz, D. J. (2013), "Cloud Workload Characterization", IETE Technical Review, 30(5), pp. 382-397.

Oriol, J. F. – Guitart, J. "Introducing Risk Management into Cloud Computing", https://upcommons.upc.edu/bitstream/handle/2117/15944/Fito.pdf?sequence=1, (26.11.2021).

Oscar, R. - Daniel, M. - Eduardo, F. M. (2015), "Empirical Evaluation of A Cloud Computing Information Security Governance Framework", Information and Software Technology, 58(2), pp. 44-57.

Özyiğit, Hüseyin (2021), Bağımsız Denetim Odaklı Kurumsal Risk Yönetimi Sisteminin Oluşturulması: İşletmelere Yönelik Model Önerisi, Gazi Kitabevi, Ankara.

PwC, (2004), "7th Annual Global CEO Survey Managing Risk: An Assessment of CEO Preparedness", New York.

Ramgovind, S. - Eloff, M. M., - Smith, E. (2010), "The Management of Security in Cloud Computing", Information Security for South Africa (ISSA), Sandton, South Africa, pp. 1-7.

Rasheed, H. (2014), "Data and Infrastructure Security Auditing in Cloud Computing Environments", International Journal of Information Management, 34(3), pp. 364-368.

Ryan, M. D. (2013), "Cloud Computing Security: The Scientific Challenge, and A Survey of Solutions", The Journal of Systems and Software, 86(9), pp. 2263–2268.

Samer, A. - Mufleh, A. - Wa'el, H. (2017), "Implementing Risk Management Processes into a Cloud Computing Environment", International Journal of Web Portals, 9(1), pp. 1-12.

Shi, Y. - Meng X. – Zhao, J. - Hu X. - Liu B. - Wang H. (2010), "Benchmarking Cloud-Based Data Management Systems", In: Proceedings of the 2nd International CIKM Workshop on Cloud Data Management, pp. 1-8.

Shigeaki, T. - Manami, H. – Motoi, I. – Hiroyuki, S. – Atsushi, K. (2011), "Risk Management on the Security Problem in Cloud Computing", First ACIS/JNU International Conference on Computers, Networks, Systems, and Industrial Engineering, pp. 1-6.

Xiang, Y. - Martino, B. D. - Wang, G. L. (2015), "Cloud Computing: Security, Privacy and Practice", Future Generation Computer Systems, 52(11), pp. 59-60.

Yao, Z. Q. - Xiong, J. B. - Ma, J. F. (2013), "Access Control Requirements for Structured Document in Cloud Computing", International Journal of Grid and Utility Computing, 4(2), pp. 95-102.

Yavuz, Selahattin - Özyiğit, Hüseyin (2018), "Kurumsal Risk Yönetimi ve Firma Performansı: Bankacılık Sektörüne Yönelik Bir Araştırma", 1. Uluslararası Bankacılık Kongresi, ss. 769-778.

Zhu, X.D. - Li, H. - Li, F.H. (2013), "Privacy-Preserving Logistic Regression Outsourcing in Cloud Computing", International Journal of Grid and Utility Computing, 4(2), pp. 144-150.

https://www2.deloitte.com/global/en.html (14.08.2021).