Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi
Yıl: 2024 Cilt-Sayı: 17(3) ss: 667-690

Academic Review of Economics and Administrative Sciences
Year: 2024 Vol-Issue: 17(3) pp: 667-690

https://dergipark.org.tr/tr/pub/ohuiibf

Araştırma Makalesi
Research Article

ISSN: 2564-6931
DOI: 10.25287/ohuiibf.1482734
Geliş Tarihi / Received: 12.05.2024
Kabul Tarihi / Accepted: 28.06.2024
Yayın Tarihi / Published: 31.07.2024

BULUT GÜVENLİK DENETİMİ: BULUT SİBER GÜVENLİK UYGULAMALARINDA İÇ DENETİM*

Ali KESTANE [1]
Ganite KURT [2]

Öz

İşletmelerin kimlik bilgilerinden gerçekleştirmiş oldukları faaliyetleri ve faaliyetlerini gerçekleştirme yöntemlerinden denetlenme süreçlerine kadar bütün aşamaların bulut ortama taşınması çeşitli güvenlik problemlerini gündeme getirmektedir. Bu bağlamda hali hazırda sınırlı sayıda bulut güvenlik modelleri ve standartları bulunsa da bahsedilen modeller proaktif olmaktan öte reaktif bir yapıya sahip olmalarından dolayı yeterli görülmemektedir. Siber alanların bulut uygulamalar içerisinde merkezi bir konuma yerleşmesi, işletmelerin iç denetim faaliyetlerinin; kim tarafından, nasıl, hangi yöntemlerle, nasıl yetenekler bağlamında yerine getirilmesi gerektiği sorularını gündeme getirmektedir. Dolayısı ile bu çalışmada bulut güvenlik uygulamalarının denetlenmesinde iç denetimin rolünün ve gelecekte ki yapısının nasıl olacağına açıklık getirilmesi amaçlanmıştır. Pratikte siber alanlar ile bulut uygulamalar geniş bir alana yayılmış olsa da iç denetim çerçevesinde yapılan çalışmaların sınırlı olduğu görülmektedir. Erişim güçlüğü yaşanması ve Türkiye'de bahsedilen uygulamaların sınırlı kullanımından dolayı bu çalışma teorik bir perspektiften ele alınmıştır. Gelecekte iç denetim açısından yapılması gerekli görülen uygulamalara yönelik öneriler getirilmiştir.

Anahtar Kelimeler ***:*** *Bulut-Siber Güvenlik, Güvenlik Denetimi, İç Denetim.*

JEL Sınıflandırması ***:*** *O30, M40, M42*

* Bu çalışma, 01-04 Kasım 2023 tarihlerinde düzenlenen VII. Uluslararası Muhasebe ve Finans Sempozyumu'nda sözlü olarak sunulan "Bulut Güvenlik Denetimi: Bulut Siber Güvenliğinin Güçlendirilmesinde İç Denetim" başlıklı bildiriden üretilmiştir.

[1] Doç. Dr., Kilis 7 Aralık Üniversitesi İktisadi ve İdari Bilimler Fakültesi, alikestane@kilis.edu.tr, ORCID: 0000-0002-7049-0354.
[2] Prof. Dr., Hacı Bayram Veli Üniversitesi Finansal Bilimler Fakültesi, ganite.kurt@hbv.edu.tr, ORCID: 0000-0001-6438-2501.

***Alıntı/Citation (APA 6)*:**
Kestane, A., & Kurt, G. (2004). Bulut güvenlik denetimi: Bulut siber güvenlik uygulamalarında iç denetim. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 17*(3), 667-690. http://doi.org/10.25287/ohuiibf.1482734.

Kestane, A., & Kurt, G. (2004). Bulut güvenlik denetimi: Bulut siber güvenlik uygulamalarında iç denetim. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 17*(3), 667-690.

CLOUD SECURITY AUDIT: INTERNAL AUDIT IN CLOUD CYBER SECURITY APPLICATIONS

Abstract

Moving all stages of businesses, from their identity information to their activities and methods of carrying out their activities to their auditing processes, to the cloud environment brings various security problems to the agenda. In this context, although there are currently a limited number of cloud security models and standards, the mentioned models are not considered sufficient because they have a reactive structure rather than a proactive one. The placement of cyberspaces in a central position within cloud applications, the internal audit activities of enterprises; It raises the questions of who, how, by what methods, and in the context of capabilities. Therefore, in this study, it is aimed to clarify the role and future structure of internal audit in auditing cloud security applications. In practice, although cyberspace and cloud applications have spread over a wide area, it is seen that the studies carried out within the framework of internal audit are limited. Due to the difficulties of access in practice and the limited use of the applications mentioned in Turkey, this study has been discussed from a theoretical perspective. Suggestions have been made for the practices deemed necessary in terms of internal auditing in the future.

Keywords *: Cloud-Cyber Security, Security Audit, Internal Audit.*

JEL Classification *: O30, M40, M42*

GİRİŞ

Siber teknolojinin hızlı bir gelişme göstermesi sonucunda bulut uygulamalar ortaya çıkmıştır. Veri ve bilgilerin korunması konusunda alınan önlemler artmış, bu durum ise tehdit ve saldırılara karşılık sistem güçlendirmesi çalışmalarının başlatılmasına yol açmıştır. Verilerin korunmasından sistemlerin işlerliğinin güçlendirilmesine kadar geniş bir alanda varlığını gösteren siber güvenlik kavramı, günümüzde yaşam alanının merkezine yerleşmiştir (Li vd. 2019: ix). Dinamik süreci açığa vuran insan yaşamı; risklerin azaltılmasına yönelik siber güvenlik bilgi sistemlerinin kurulmasını olmazsa olmaz hale getirmektedir (Wyatt, 2017: 336).

Siber teknoloji paralelinde ortaya çıkan bulut uygulamalar yaşamın hemen her alanını ele geçirmiş durumdadır. Eğitimden teknik alanlara, sosyo-kültürel alanlardan yasal düzenlemelere kadar birçok alanı etkilemektedir. Yaşam alanını etkisi altına alan ve iş dünyası içerisinde farklı alanlarda kullanım alanına sahip olan bulut uygulamaların; denetim çalışmalarının gerçekleştirilmesini nasıl etkileyebileceği önemli merak konusu olmuştur. Teknoloji kullanımından hareketle işletmelerin faaliyetlerinin dijital platformlara taşınması gerçekleştirilen faaliyetlerin denetlenmesinin nasıl olacağı sorusunu gündeme getirmiştir. Dolayısı ile bu çalışmada bulut güvenlik uygulamalarının denetlenmesinde iç denetimin rolünün ve gelecekte ki yapısının nasıl olacağına açıklık getirilmesi amaçlanmıştır. Dijital dünyanın somut gerçeklerinin ortaya koyulması, bulut güvenliği bağlamında iç denetim faaliyetlerinin gelecekteki yapısı ve rolüne açıklık getirilmesi bu çalışmanın özgün değerini ve önemini ortaya koymaktadır. Çalışmanın amacı ve önemi bağlamında bulut uygulamaları ve siber güvenlik konularına açıklık getirilmesi ve iç denetim çalışmalarının mevcut durumundan geleceğe nasıl yol alınabilir sorusuna yanıt olarak betimsel içerik analizi yöntemi benimsenmiştir. Yapılan değerlendirme neticesinde iç denetiminin rolünün belirlenmesi konusunda çözüm önerileri getirilmiştir.

Çalışma iki ana bölüm üzerinden organize edilmiştir. Birinci bölümde; i) kavramsal çerçeve (siber alan, siber güvenlik, bulut güvenlik modelleri), ii) bulut denetim literatürü ve bulut güvenlik standartları ve iii) bulut güvenliğinde karşılaşılan problemler ele alınmıştır. İkinci bölümde; i) bulut uygulamalarında bilgi güvenliği denetim süreci, ii) görevler ayrılığı ve iii) bulut güvenliğin güçlendirilmesinde iç denetim rolünün tespit edilmesine odaklanılmıştır. Son olarak mevcut durum tartışması yapılarak gelecekte atılması gereken adımlara ilişkin öneriler sunulmuştur.

I. KAVRAMSAL ÇERÇEVE

Bulut güvenlik denetiminin, çalışmanın anatomisine uygun olarak açıklanması bakımından; *i) siber alan, ii) siber güvenlik* ve *iii) bulut güvenlik modelleri* gibi temel kavramların açıklığa kavuşturulmasında yarar görülmektedir.

I.II. Siber Alan

Siber alan kavramı hakkında farklı araştırmacılar tarafından değişik tanımlamaların yapıldığı görülmektedir. Araştırmacıların bir kesimi siber uzay kavramını kullanırken diğer kesimin siber alan kavramını kullandıkları görülmektedir. Bu araştırmanın teması bağlamında siber alan kavramının nasıl kullanıldığının belirtilmesinde yarar görülmektedir. Uluslararası Telekomünikasyon Birliği tarafından en geniş ve güncel tanımı ile ifade edilen siber alan; halka açık ya da özel kesimden kullanıcıları, interneti, kendisine bağlı bilgi işlem cihazlarını ve internete doğrudan veya dolaylı olarak bağlanabilen tüm uygulama, hizmet ve sistemleri ile birlikte yeni nesil ağ ortamını kapsamaktadır. Yapılan tanımdan hareketle siber alanın; kullanıcıları olduğu kadar bilgi işlem öğelerini, kaynakları ve birbirine bağlanan altyapıyı da kapsadığı anlaşılmaktadır (ITU, 2023).

Farklı ülkeler siber güvenlik stratejilerinde siber alanı, dar anlamda ifade edebilmektedir. Avustralya'nın Siber Güvenlik Stratejisine (Australia Government, 2013) göre, siber alan; bilgisayar sistemlerinin güvenliğini ifade etmektedir. Bahsi geçen ifade siber alanın sadece bilgisayar sistemlerinden ibaret olduğunu göstermekte ve pek çok unsurun dahil edilmediği anlamına gelmektedir. Kanada'nın Siber Güvenlik Stratejisine (Canada Government, 2010) göre, siber alan, birbirine bağlı bilgi teknolojisi ağları ve bu ağlardaki bilgiler tarafından yaratılan elektronik dünyayı ifade etmektedir. İnsanların fikir, hizmet ve dostluk alışverişinde bulunmak için birbirine bağlandığı küresel bir ortak noktadır. Hollanda Ulusal Siber Güvenlik Stratejisine (Holland Government, 2013) göre, siber alan, Bilgi ve İletişim Teknolojilerinin (BİT) kesintileri, arızaları veya kötüye kullanımından kaynaklanan hasarları önleme çabalarını ifade etmektedir. Bu bağlamda siber alan, BİT alanındaki her şeyi kapsamaktadır. Almanya'nın Siber Güvenlik Stratejisine (Germany Government, 2011) bakıldığında ise siber alan, küresel ölçekte veri düzeyinde birbirine bağlı tüm BT sistemlerinin sanal alanı olarak ifade edilmektedir. Diğer taraftan Yeni Zelanda'nın Siber Güvenlik Stratejisine göre; siber alan, internet gibi küresel bir ağ olarak kabul edilmektedir (New Zealand Government, 2015). Siber alanın tanımı, görüldüğü üzere farklı ülkelerde farklı ifadeler ile karşılık bulmakta bu durum ise siber güvenlik tanımlarında da farklı vurgulara yol açmaktadır.

Siber alanın kavramsal açıklamasından hareketle unsurlarına bakıldığında ise Rajnovic (2012) siber alanın; somut, soyut ve ağla ilgili öğelerden oluştuğunu buna karşılık Ottis ve Lorents (2010) ise siber alanın zaman ve insandan ibaret olduğunu ifade etmiştir. Söz konusu tanımların özüne bakıldığında insanın ve etkileşimin siber alanın merkezinde yer aldığını göstermektedir.

Siber alanı, zamana bağlı birbirine entegre bilgi sistemleri ve bu sistemlerle etkileşime giren insan kullanıcıları olarak tanımladılar. Bu tanımla insan ve etkileşim siber alanın işleyişinin merkezinde yer almaktadır.

I.II. Siber Güvenlik

Siber güvenlik kavramı Gasser (1988) tarafından siber güvenlik ya da BT güvenliği olarak da bilinen bilgisayar güvenliği, bilgi sistemlerinin hırsızlığa ya da donanıma, yazılıma ve bunlara ilişkin bilgilere zarar gelmesine ve kesintiye uğramasına karşı korunması olarak ifade edilmektedir. Craign ve diğerleri (2014), siber güvenliği; siber alanı ve organizasyonu korumak için kullanılabilecek araçlar, politikalar, güvenlik kavramları, güvenlik önlemleri, yönergeler, risk yönetimi yaklaşımları, eylemler, eğitimler ve en iyi uygulamalar ile güvence ve teknolojilerin toplamı olarak tanımlamaktadır. Bahsedilen ifadelerden; bilgi güvenliğinin bilginin gizliliğine (Kurt ve Uysal, 2015), bütünlüğüne ve kullanılabilirliğine vurgu yaptığı, bilgisayar güvenliğinin ise sistemlerin kullanılabilirliğine, bütünlüğüne ve doğru çalışmasına odaklandığı açıktır. Bununla birlikte siber güvenliğin; araçların,

süreçlerin, kavramların ve içindeki unsurlar arasındaki gerekli etkileşimin kullanılmasıyla kuruluşun tüm varlıklarının korunmasını vurgulaması bakımından daha kapsamlı olduğunu belirtmek yararlı olacaktır.

Siber güvenlik, siber alanın bütün unsurlarıyla; i) yetkisiz erişiminden ve etkileşimden korumakla birlikte ii) gizliliğini ve bütünlüğünü korumak ve iii) koruma amaçlı kullanılan sistemler, araçlar, süreçler, uygulamalar, kavramlar ve stratejiler toplamı olarak düşünülebilmektedir. Bahsedilen tanımdan hareketle siber güvenliğin kapsamının üç açıdan netleştiği açıktır. İlk olarak, daha dar anlamda güvenlikten ziyade siber alanın güvenliğine dikkat çekmek için bilgi güvenliği ya da BT güvenliği terimleri yerine siber güvenlik terimi kullanılmaktadır. İkincisi, sadece koruma değil, önleme de siber güvenliğin ayrılmaz bir parçasıdır. Güvenliğe, önleme ve korumanın birbiriyle ilişkili olduğu daha geniş bir bağlamda bakılabilmektedir. Bazı güvenlik açıklarının suistimal edilmesini önlemek, alanı korumak olarak değerlendirilebilirken, siber ortamın nasıl korunacağını bilmek, bir ölçüde güvenlik ihlallerinin nasıl meydana geldiğini ve nasıl önlenebileceğini de bilmek anlamına gelmektedir. Üçüncüsü, bulut, nesnelerin interneti ve sosyal ağlar gibi birçok modern teknolojinin hızla ortaya çıkmasıyla birlikte, CIA'nın üçlü kurallarına (Gizlilik, Bütünlük ve Kullanılabilirlik) karşılık siber güvenlik kavramı anlam bulmaktadır. Günümüzde, yeni ve gelişmekte olan teknolojilerle değişmez bir model elde etmek için, özgünlük, hesap verebilirlik ve güvenlik gibi ilave özelliklerin tanımlamaya dahil edilmesi önemli görülebilmektedir (Le ve Hoang ,2017: 4).

I. III. Bulut Güvenlik Modelleri

Bulut belirli bir siber alanı ifade etmektedir. Sanallaştırmaya ve paylaşılan BT kaynaklarına dayanan bulut bilişim, siber alanın teknolojik bir evrimi olarak kabul görmektedir. Dünya BT gelişiminde önemli bir rol oynamaktadır (Lacity, 2012: 6). Ancak siber altyapılar olarak bulutlar; üç hizmet modeli (hizmet, platform/süreç ve altyapı) ve dört dağıtım bulutu türü (Özel, Kamu, Hibrit ve Bütünleşik) ile zorlu güvenlik sorunlarıyla karşı karşıya kalmaktadır. IDC araştırmasına göre, CIO'ların %74'ünün bulut bilişimle ilgili en büyük sorunu güvenlik olarak öne çıkmaktadır (Clavister, 2008).

Tanımlanan bulut güvenliği yönleri arasında yönetişim ve uyumluluk, sanallaştırma, kimlik yönetimi (Behl ve Behl, 2012; Catteddu, 2010; Coucil, 2015) ve çeşitli tehdit yönleri (Claycomb ve Nicoll, 2012; Farhan ve Haider, 2011) yer almaktadır. Bulut Güvenliği Birliği (Cloud Security Alliance-CSA), kuruluşlara isabetli risk yönetimi kararları alma konusunda bulut güvenliği sorunları hakkında farkındalık sağlayan "The Treacherous Twelve Cloud Computing Top Threats" isimli güvenlik raporunu 2016 yılında yayınlamıştır (Alliance, 2016).

Bulut güvenliği sorunlarıyla mücadele etmek için araştırmacılar, işletmeler ve kuruluşlar, bulut güvenlik standartları ve modelleri geliştirerek bulut güvenliği riskini azaltmak ve güvenlik tehditleriyle mücadele etmek için çaba harcamaktadır. Avrupa Birliği Ağ ve Bilgi Güvenliği Ajansı (ENISA, 2014) 2014 yılında, bulut bilişim güvenliğiyle ilgili standartlara genel bir bakış sağlamak için Bulut standartları ve güvenliği raporunu yayınlamıştır. Bulut Güvenliği Birliği, 2009 yılında Sürüm 1.0 (Archer and Boehm, 2009), Sürüm 2.1 (Brunette and Mogull, 2009) ve 2011 yılında Sürüm 3.0 (Alliance, 2011) olmak üzere 3 sürüm aracılığıyla bulut bilişimdeki kritik odak alanları için güvenlik rehberliğini sunmuş ve geliştirmiştir. En son sürüm (Sürüm 3.0), güvenlik talebindeki değişikliği karşılamak için tasarlanmıştır. İlgili rehberin amacı, kuruluşların güvenlik etki alanlarını uygulayarak bulut için siber güvenliği yönetmelerine yönelik daha iyi standartlar sunmaktır. Rehber, bulut mimarisine yönelik bulut hizmeti modeli (SaaS, PaaS ve IaaS) ve özel gereksinimleri karşılayan türev varyasyonlarla dört dağıtım modeli (Kamu, Özel, Karma ve Hibrit Bulut) ile yapılandırılmıştır. Rehberin temeli yönetişim ve operasyonel olmak üzere iki genel kategori altında on üç farklı alana dayanmaktadır. Yönetişim alanları, bulut bilişim ortamındaki politikaların yanı sıra geniş ve stratejik konulara odaklanırken, operasyonel alanlar daha taktiksel güvenlik kaygılarına ve mimari içindeki uygulamaya odaklanmaktadır.

Rehber, bulut bilişim, hizmet modelleri ve dağıtım modellerine açıklık getirmektedir. Bulut güvenliği yönetimiyle ilgili olarak, rehber buluta özgü; i) birlikte çalışabilirlik ve taşınabilirlik, ii) veri güvenliği ve iii) sanallaştırma gibi konulara odaklanmaktadır. Uygulama alanlarının stratejik ve taktik kategorilere göre iki gruba ayrılması rehberin bir diğer dikkat çeken noktasıdır. Bu yaklaşım, bulut tüketicilerinin ve sağlayıcılarının finans ve insan kaynaklarının güvenliğini dikkate almalarına olanak

tanımaktadır. Ayrıca, Bulut Kontrol Matrisi (Swain vd., 2010: 14), uluslararası siber güvenlik standartları ISO/IEC 27002 ve diğer NIST Özel Yayınları gibi mevcut güvenlik modelleriyle eşleştirilmelerine imkân vermektedir. Bununla birlikte, faydalarına rağmen rehberin birtakım dezavantajları da bulunmaktadır. Rehberde her bir alan için değerlendirme adımları bulunmamaktadır. Güvenlik uygulamaları için güvenlik ölçümleri dikkate alınmamaktadır. Bu nedenle kuruluşlar bir alan adının güvenlik düzeyini belirlemekte zorlanmaktadır.

Bulut güvenliğine ilişkin standartlar da bulunmaktadır. ISO/IEC 27017 Standardı, bulut bilişimin bilgi güvenliği unsurlarını göstermektedir. Bulut bilişimin gizlilik yönlerine ilişkin ISO/IEC 27018, iş sürekliliğine ilişkin ISO/IEC 27031 ve ilişki yönetimi üzerine ISO/IEC 27036-4 dahil olmak üzere ISO 27000 serisi standartları ile birlikte buluta özgü bilgi güvenliği kontrollerinin uygulanmasına yardımcı olmaktadır. Ulusal Standartlar ve Teknoloji Enstitüsü (NIST), bulut bilişimle ilgili olarak; i) NIST SP 500-291, Bulut Bilişim Standartları Yol Haritası, ii) NIST SP 800-146, Bulut Bilişim Özeti ve Önerileri, iii) NIST SP 800-1, Genel Bulut Bilişimde Güvenlik ve Gizlilik Yönergeleri, iii) NIST SP 500-292, Bulut Bilişim Referans Mimarisi ve iv) NIST SP 500-293, ABD Bulut Bilişim Teknolojisi Yol Haritası standartlarını yayınlamıştır.

I.IV. Bulut Denetim Standartları ve Çerçeveleri

Standartlar, denetim süreçlerinin geliştirilmesinde çok önemli bir role sahip olan bazı normların, özelliklerin ve uygulama çerçevelerinin uygulanmasında tekdüzelik sağlama rolüne sahiptir. Bulut teknolojilerinin hızlı gelişimi, kullanıcılara makul güvence sağlamak üzere tüm BHS'ler için geçerli standartların elde edilmesini tetiklemektedir.

Tüm donanım ve yazılım bileşenleri, kuruluşun yönetiminde olduğu; geleneksel BT altyapıları, güvenliğin tüm bileşenlerini ve hedeflerini amaçlayan karmaşık ve ayrıntılı denetim süreçlerinin geliştirilmesine olanak tanımaktadır. Aralarında (BKM) Bulut Kontrolleri Matrisi, ISACA (Bilgi Sistemleri Denetim ve Kontrol Birliği) - Bulut Bilişim Denetim Programı, ENISA (Avrupa Ağ ve Bilgi Güvenliği Ajansı) vb. sayabileceğimiz bulut teknolojilerine özgü çerçeve ve standartlar geliştirmiş çeşitli kuruluşlar bulunmaktadır. Bu standartlardaki ana güvenlik yönergeleri ve kavramları aşağıdaki gibidir (Rissi and Sherman, 2011: 17-20):

- Bulut tabanlı sistemler özel güvenlik yöntemlerine ihtiyaç duymakta ve geleneksel yöntemler yeterli görülmemektedir.
- Denetçiler, kuruluşun bulut sistemlerinde her zaman gerekçelendirilmeyen, kaynak israfını temsil eden birden fazla geleneksel kontrol mekanizması biriktirdiğini ve bunların ortadan kaldırılması gerektiğini tespit edebilmektedir.
- Denetim sürecinin sağlıklı bir biçimde yürütülebilmesi için denetçilerin bellek dosyaları, kimlik yönetimi, erişim kontrolü gibi temel hizmetlerin yanı sıra bulutta kullanılan yeni güvenlik kontrolleri hakkında da detaylı bilgi sahibi olması gerekmektedir.
- Denetimin amacını belirlemek, bünyesinde yer alan ya da kiralanan sistemlere bağlantılar gerektirmesinden dolayı bulut topolojisine özgü mimariler hakkında sağlam bilgi gerektirmektedir.

Bulut altyapısında standartların uygulanması kullanıcılar için ek bir güvence sağlamış olsa da en önemli güvenlik tehditlerinden bazıları ek güvenlik kontrollerine ihtiyaç duymaktadır. DoS (Denial of Service), Kötü Amaçlı Yazılım Enjeksiyon Saldırısı, Kimlik Doğrulama ve MiTM Saldırısı gibi saldırılar ancak derinlemesine savunma mekanizmalarının uygulanması ve bu zorlukların üstesinden gelebilecek bütünsel ve üniter bir güvenlik stratejisinin benimsenmesiyle durdurulabilecektir.

Bulut siber güvenliğinde içinde bulunduğumuz dönem itibari ile yapay zekâ uygulamalarına geçildiği açıkça görülebilmektedir. Fakat bu aşamada bulut güveliği standartlarından bahsetmek çalışmanın teması bakımından önemli kabul edilmektedir. Yakın geçmişte bulut güvenliği standartları

üzerinde çalışan çok sayıda kuruluş bulunmaktadır. Kapsamlı olmayan aşağıdaki liste, bugün gelişmekte olan standartlar üzerinde çalışan kuruluşların çeşitliliği hakkında bir fikir vermektedir. Söz konusu kuruluşlar (Duncan ve Whittington, 2016): AICPA, ARTS, Basel 3, BITS, CSA, CSCC, COBIT, CSO, DPA, DMTF, ETSI, FedRamp, Generally accepted privacy principles (GAPP), GICTF, HIPA, IATAC, ISACA, ISAE 3402, ISO/IEC, ITIL, ITU, Jericho Forum, NIST, NERC, OASIS, OCC, OGF, OMG, PCIDSS, SNIA, The Open Group ve TM Forum şeklindedir.

Bahsedilen kuruluşların çoğu, özellikle üyelerinin bulut hizmetlerini daha güvenli bir şekilde nasıl kullanabilecekleriyle ilgili olabilecek belirli bulut alanlarını ele almıştır. Örneğin PCIDSS, bulutun ödeme mekanizmaları üzerindeki etkileriyle özel olarak ilgilenmektedir. CSA, ISACA, ISO/IEC, NIST gibi daha büyük kuruluşlar sorunun çözümüne daha geniş bir açıdan bakma eğilimindedir. CSA ve ISACA bulut odaklı kuruluşlar iken, ISO/IEC ve NIST çok daha geniş bir odağa sahiptir. Son iki kuruluştan NIST bir bulut güvenlik standardı üretmekte çok hızlı davranırken, ISO/IEC standartlarının onay süreci çok yavaştır. Bir ISO/IEC standardı onaylandıktan sonra genellikle büyük küresel şirketler tarafından benimsenebilmektedir. Bu süreci örneklendirmek gerekirse, NIST ilk bulut standardını 2009 yılında yayınlamış, bunu 2011 yılında ABD şirketleri tarafından benimsenen daha kapsamlı bir standart izlemiştir. Oysa ISO/IEC'nin buluttan bahsetmesi bile 2014 yılını bulmuştur.

Bulut güvenlik standartlarının dünya genelinde ki yapısal oluşum sürecini takiben bulut güvenliği konusunda karşı karşıya kalınan problemlerin açıklığa kavuşturulması önemli görülmektedir. Karşılaşılan problemler ve bulut güvenliğinin zorlukları aşağıda açıklanmaktadır.

İyi bir güvenlik hedefine ulaşmak için ele alınması gereken bir dizi zorluk vardır. Bilgi güvenliğinin temel kavramları gizlilik, bütünlük ve erişilebilirliktir (CIA); bu kavramlar, işletme yönetiminin bir şirketi vekalet teorisi altında yönetmesinin yaygın bir uygulama olduğu zamanlarda geliştirilmiş bir çerçevedir. Vekalet teorisinin kurumsal açgözlülüğün aşırılıklarını engellemekte nasıl başarısız kaldığı bilinmektedir. Benzer durumun bulut güvenliğine uygulandığında da geçerli olduğu görülmektedir. Dolayısıyla farklı bir yaklaşıma ihtiyaç duyulduğu anlaşılmaktadır. Önemli görülen 10 (on) temel güvenlik sorunu öne çıkmaktadır (Duncan ve Whittington, 2014; Duncan ve Whittington, 2015a, 2015b; Duncan ve Whittington, 2016):

- Güvenlik hedeflerinin tanımı
- Standartlara uygunluk
- Denetim sorunları
- Yönetim yaklaşımı
- Bulutun teknik karmaşıklığı
- Sorumluluk ve hesap verebilirlik eksikliği
- Ölçme ve izleme
- Yönetimin güvenlik konusundaki tutumu
- Şirketteki güvenlik kültürü
- Tehdit ortamı

Güvenlik hedeflerinin tanımına bakıldığında, kurumsal yönetim kuralları gibi iş ortamının da sürekli değiştiğini ve bunun da güncel kalmak için değişen güvenlik önlemlerine ihtiyaç duyulacağı anlamına geldiği görülmektedir. Birçok yönetici uygun güvenlik hedeflerinin nasıl tanımlanacağı konusunda yetersiz, isteksiz ya da emin değildir (Papanikolaou vd., 2011: 3; Baldwin vd., 2013; Duncan ve Whittington, 2015c). Artık sorumluluk ve hesap verebilirlik (Huse, 2005), sosyal vicdan (Gill, 2008), sürdürülebilirlik (Ioannidis vd., 2013; Kolk, 2008), esneklik (Chapin vd., 2009) ve etik (Arjoon, 2012) konularına daha fazla vurgu yapılmaktadır. Sorumluluk ve hesap verebilirlik aslında diğer tüm güvenlik hedeflerine ulaşmaya yardımcı olmak için kullanabilecek mekanizmalardır. Güvenlik hedeflerinin tanımını genişletmek, başarılı bir bulut denetimine ulaşmak için daha etkili bir yol sağlayabilmektedir.

İyi bir bulut güvenliğinin önünde; standartlara uygunluk, yönetim yaklaşımı ve karmaşıklık biçiminde üç önemli engel bulunmaktadır. Tutarlı bulut standartlarının eksikliği, bulut denetiminin

etkinliğini zayıflatmanın yanı sıra bu süreçte kontrol listelerinin kullanılamaması gibi temel bir zayıflık ortaya çıkarabilmektedir (Duncan ve Whittington, 2015a). Karmaşıklık ise ölçme ve izleme ile birlikte değerlendirilebilmektedir.

Uygulamada bulut güvenlik standartlarına uyumun sağlanması konusunda, uyum ve denetim yoluyla güvenliğin sağlanması için güvence önemli kabul edilmektedir. İlk olarak uyumluluk konusuna değinilecek olursa, ele alınması gereken bir dizi zorluk bulunmaktadır. Bulut bilişimin evriminden bu yana, bir dizi bulut güvenlik standardı geliştirilmiştir. Fakat sorun şu ki, uygulamada hala tam güvenlik sunan bir standart bulunmamaktadır. Bulut uygulamalarında güvenliğin sağlanması konusunda "Tek beden her şeyi kapsar", denilebilecek bir standardın olmaması farklı bir dezavantaj oluşturmaktadır (Duncan ve Whittington, 2014). Yeni teknolojinin gelişim hızı, uluslararası standart kuruluşlarının değişikliklere ayak uydurma kapasitesini çok aşmaktadır (Willingmyre, 1997: 5). Bu da sorunu daha da derinleştirmekte ve yakın zamanda çözülemeyebileceği anlamına gelmektedir. İşletmelerin uyum sorunları ele alınırken standartlardaki bu boşlukları dikkate almaları gerektiği açıktır. Yalnızca uyumluluğa güvenmek etkin güvenliğe zarar verebilecektir. Bu bağlamda standartların kural temelli yaklaşımdan risk temelli yaklaşıma doğru hareket etmesi beklenmektedir. (Humphreys, 2008; Albersmeier vd., 2009; Prislan ve Bernik, 2010: 61; ISECT, 2011; Baldwin vd., 2013; Order, 2013).

Bulut denetiminin olgunlaşmış bir alan olmadığı ve bulut denetimine ilişkin ilk çalışmaların çoğunun teknik sorunların ele alınmasına odaklandığı bir gerçektir. Uzun zamandır sadece teknik konulara odaklanmanın bulut güvenliğini asla çözemeyeceği görüşü bulunmaktadır. Bir işletmenin iş mimarisi yalnızca teknolojiden değil insan, süreç ve teknolojiden oluşmaktadır (PwC, 2016). Dolayısıyla yalnızca teknik bir çözüme odaklanmanın güvenliği zayıflatması muhtemeldir. Bu noktada yönetimin, denetimin amacını ve önemini daha iyi anlaması (Sang, 2013: 92) ve denetim izinin sunduğu kilit önem ve zayıflıklarını da anlaması önemli kabul edilmektedir (Duncan ve Whittington, 2016a).

Yönetim yaklaşımının, bulut ekosistemindeki karmaşık ilişkileri ele alırken dikkat edilmesi gereken önemli bir husus olduğuna şüphe yoktur (Duncan ve Whittington, 2015d). Tüm aktörler aynı yaklaşımı kullanmasa da yönetimin kendi bulut ekosisteminde yer alan aktörlerin her biri tarafından kullanılan yönetim yaklaşımını tanıması kesinlikle yararlı olacaktır.

Çok sayıda bulut kullanıcısı, bulutun kullanımı basit bir paradigma olduğu görüşünü benimsemekte, ancak bulutun karmaşıklığının yarattığı ciddi etkinin farkında olmamaktadır. Yeni teknolojinin getirdiği artan karmaşıklık, bu risklerin öneminin kavranamamasının bir sonucu olarak riske maruz kalma potansiyelinin artmasına neden olmaktadır (Zio, 2009: 131). Diğer taraftan bulut, bir kullanıcının, örneğin bir veri tabanı arka ucuna sahip bir web sunucusunu, genellikle bir dizi zayıflığı ortaya çıkarabilecek varsayılan ayarlara güvenerek hızlı bir şekilde dağıtmasına olanak tanımaktadır (Duncan ve Whittington, 2016b). Varsayılan ayarlar genellikle kullanılabilirliğe güvenlikten çok daha fazla önem vermektedir.

Kurumsal Sosyal Sorumluluk (CSR) ölçümü üzerine çok sayıda araştırma yapıldığı bilinmektedir, ancak etkili önlemlerin düzgün bir şekilde geliştirilmesi ve uygulanması için hala kat edilmesi gereken yollar olduğu açıktır. Ölçüm son derece önemli olmakla birlikte, bunu başarmak çok zor olabilmektedir. Güvenlik yönetimi söz konusu olduğunda sürekli izleme yönteminin kullanılmasına açık bir ihtiyaç vardır. Küresel güvenlik şirketlerinin hem bulut dışı hem de bulut verilerini kapsayan raporları (PwC, 2012; Trend, 2012; Verizon, 2012), güvenlik ihlallerinin %85'inden fazlasının, genellikle anlayış eksikliği, yetkinlik eksikliği veya mağdurların sistemlerinin kötü yapılandırılmasıyla kolaylaştırılan düşük düzeyde teknik yeterlilikten ileri geldiğini göstermektedir.

Önemli bir süredir, yönetimin güvenlik konusundaki tutumu yüksek bir öncelik olmuştur (ISACA, 2009). Güvenlik profesyonellerinin %77'si güvenlik tutumlarının en tepeden belirlenmesi gerektiğini vurgulamaktadır. Bir rapora göre (PwC, 2012), yöneticileri dinlediğinizde yönetimin tutumu yüksek, BT uygulayıcılarını dinlediğinizde ise düşüktür. Bu nedenle yönetimin, bunun sadece teknik bir mesele olmadığının, aksine kurumun en tepesinden yönlendirilmesi gereken temel bir iş süreci olduğunun tam olarak farkında olması gerekmektedir. Bilgi güvenliği günümüzde iş dünyasının karşı karşıya olduğu en büyük risklerden biridir ve gereken ilgi ve bağlılığın gösterilmesi gerekmektedir.

Bir şirkette iyi bir güvenlik oluşturmanın en önemli unsurlarından biri, kurum içinde iyi bir güvenlik kültürünün geliştirilmesi ve sürdürülmesidir (ISACA, 2009; PwC, 2010, PwC 2012,).

Günümüz itibariyle maliyetlerin ve güvenlik sorunlarının artmasına bağlı olarak özellikle de gelişen teknoloji ile birlikte bulut hizmet sağlayıcıları üzerinden hizmet sunan kurumların sayısı artış eğilimi göstermektedir (PwC, 2024). Fakat bu aşamada elde edilecek başarı üst yönetimin güvenlik konusunda sergilediği tutuma bağlıdır. Bu tutum, personelin güvenlik tehditleriyle nasıl başa çıkacağını anlamasını sağlamak için uygun personel eğitimiyle birleştirilebilmektedir.

Tehdit ortamının, endüstrinin karşılaştığı teknolojik değişiklikler kadar hızlı geliştiği açıktır. Bunun yarattığı tehdidin farkında olunması, içeriden gelen tehditlerin de önemli bir güvenlik riski oluşturduğunun bilincine varılması ve olası etkiyi en aza indirmeye çalışılması gerekmektedir. Saldırganlar üzerinde hiçbir kontrol olmasa da hayatı onlar için zorlaştırarak etkiyi azaltmak mümkün olabilmektedir.

Yukarıdaki 10 (on) konu, şirketin güvenlik pozisyonunu belirlemekten ve bu hedeflerin yerine getirilmesini sağlamaktan sorumlu kişiler oldukları için bir şirketin yönetimi için özellikle önemlidir. Sonraki bölümlerde, bir bulut çözümünü benimserken yönetim tarafından yapılan bir dizi yaygın hatayı ele alınacaktır. Bu hatalardan bazıları oldukça basit, bazıları ise daha karmaşıktır. Ancak hepsinin ortak bir noktası vardır, hepsi de güvenliği olumsuz yönde etkilemektedir.

II. LİTERATÜR

Yukarıda bahsi geçen bulut güvenlik uygulamalarına ilişkin oluşturulan kavramsal çerçeve ve bulut standartlarından hareketle bulut denetimi üzerine yapılan ve bu çalışmanın teması kapsamında önemli kabul edilen çalışmalardan bahsetmek yararlı olacaktır. İlgili çalışmalar aşağıda açıklanmaktadır.

Vouk (2008), bulut bilişimi çevreleyen sorunların erken bir açıklamasında, süreçleri, verileri ve işlem sonuçlarını denetleme yeteneğinin olması gerektiğini öne sürmektedir. Wang ve diğerleri (2009), bulut paradigmasının henüz iyi anlaşılmamış birçok yeni güvenlik sorununu nasıl beraberinde getirdiğini ele almıştır. Araştırmacılar, bulut bilişimde veri depolamanın bütünlüğünü sağlama sorununu, özellikle de bulut müşterisi adına denetçinin bulutta depolanan dinamik verilerin bütünlüğünü doğrulamasına izin verme görevini incelemişlerdir. Araştırmacılar, zorlukları ve potansiyel güvenlik sorunlarını tanımlamakta ve bu özelliklerin protokol tasarımına sorunsuz bir şekilde entegre edilmesi için bir doğrulama şemasının nasıl oluşturulacağını ortaya koymaktadır. Leavitt (2009), Bulut Hizmeti Sağlayıcıları (BHS)'nın verilere kimin erişebildiğini ve yetkisiz personelin bilgiye ulaşmasını nasıl engelleyebildiklerini gösteremedikleri takdirde müşteri denetimlerinden geçemeyeceklerini öne sürmektedir. Bazı BHSler, sistemlerini önceden denetlemeleri için bağımsız denetçileri görevlendirerek ve müşterilerin veri güvenliği ihtiyaçlarını karşılamak üzere tasarlanmış prosedürleri belgeleyerek bu sorunu çözmeye çalışmaktadır. Denetçinin bir muhasebe firması olmadığı durumlarda, denetçinin tarafsızlığı konusunda bazı soru işaretleri olabilmektedir. Bernstein ve diğerleri (2009), "bulutlardan oluşan bir bulut" olasılığından bahsetmektedir. Ancak diğer bulutlardaki doğru sunucuya bağlanabilirliği sağlamak için kullanılan güvenlik süreçleri konusunda endişe duymaktadır. Bir tür denetime ihtiyaç duyulacağını öne sürmektedir. Araştırmacılar, bulut sistemlerinin güçlü ve güvenli denetim izleri sağlaması gerektiğini vurgulamaktadır. Pearson ve Benameur (2010), bulutta uygun denetim izlerinin elde edilmesinin çözülmemiş bir sorun olduğunu kabul etmektedir. Wang ve diğerleri (2010) bulutta veri depolama güvenliği için gizliliği koruyan genel denetimi ele almakta ve denetçinin sisteme zayıflık getirmesini önlemek istemektedir. Araştırmacılar, denetçiler tarafından kamu denetimine daha güvenli bir yaklaşım sağlamak için bir mekanizma sunmaktadır. Srinivasamurthy ve diğerleri (2013) bulut bilişimde güvenlik ve gizlilik üzerine bir anket gerçekleştirmiş ve çeşitli Bulut Hizmet Sağlayıcılarının güvenlik ve gizlilik konularındaki endişeleri hakkında araştırma yapmıştır. Araştırmacılar, bulut uygulamalarının güvenliği için beş unsurun (kullanılabilirlik, gizlilik, veri bütünlüğü, kontrol ve denetim) dikkate alınmasını önermektedir. Chen ve Yoon (2010), BT denetimi yoluyla güvenli bir bulut bilişim sağlanmasına yönelik veri akışını ve yaşam döngüsünü takip etmek ve kontrol sağlamak üzere bulut dağıtım modellerine ve bulut hizmetleri modellerine bir çerçeve oluşturmuştur. Ruebsamen ve Reich (2013) sürekli denetim işlemlerini ve raporlamalarını gerçekleştirmek için yazılım aracılarının kullanılmasını önermektedir. Bulut kullanımının dinamik

olarak değişen doğasını ele almak ve önemli kullanım dönemlerine ilişkin kanıtların gözden kaçırılmamasını sağlamak adına sürekli denetimi önermektedir. Doelitzscher ve diğerleri (2013), bulut müşterilerinin normal kullanım davranışlarını analiz etmek ve öğrenmek için sinir ağlarının kullanılmasını önermektedir. Lopez ve diğerleri (2014) dijital kanıtların toplanması konusunda gizlilik dostu bulut denetimleri önermektedir. Araştırma sonuçları, bulut denetçilerine müşteri gizliliğini koruyan denetim verileri sağlayabileceğini göstermektedir. Shameli-Sendi ve Cheriet (2014) bulut bilişim platformlarıyla ilişkili güvenlik risklerini değerlendirmek için bir çerçeve oluşturmuşlardır. Scholar ve Jayerah (2021), bulut bilişimdeki yakın tarihte meydana gelen güvenlik sorunlarını ele almıştır. Güvenlik sorunlarının giderilmesi bakımından sürekli denetim uygulamalarının hayata geçirilmesini vurgulamıştır. Kumar ve diğerleri (2022) bulut depolama işlemlerinde siber güvenlik çoklu anahtar yöntemi üzerine yapmış oldukları araştırmada nesne tanımlama hatalarını azaltmak için geliştirilmiş bir ResNet modeli ortaya koymuşlardır. Saxena ve diğerleri (2023) çoklu risk analizine dayalı bulut siber güvenliği için yapay zekâ odaklı tahmin modeli geliştirmiş oldukları çalışmada hazırlamış oldukları modelin siber güvenlik tehditlerinin yaklaşık %90 azalttığını belirtmişlerdir.

Bulut denetimi kapsamında ulusal literatürde doğrudan ilişkili olabilecek çalışmalara erişilememesinden dolayı araştırmanın teması bağlamında uluslararası literatürde yer alan çalışmalar sunulmuştur. Buradan hareketle bulut uygulamalarında bilgi güvenliği denetimine ilişkin çerçevenin açıklanmasında yarar görülmektedir.

III. BULUT UYGULAMALARINDA BİLGİ GÜVENLİĞİ DENETİMİ

Bir kuruluştaki siber güvenlik denetim programının temel amacı, bilgi teknolojisi alanındaki operasyonel süreçlerin kalite ve uyumluluk derecelerini belirlemek amacıyla doğrulamaktır. İlgili süreç; i) sistemlerin ve bilgilerin, ii) veri tabanlarının, iii) işletim sistemlerinin etkisini dikkate alan süreçlerin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak üzere tasarlanmış olup yasa ve standartlara uygun olarak savunma ve güvenlik ekipmanları gibi bileşenleri kapsamaktadır (Chou, 2015: 141). ISO denetimi, "kalite faaliyetleri ve buna bağlı sonuçların planlanan düzenlemelere uygun olup olmadığını ve bu düzenlemelerin etkin bir şekilde uygulanıp uygulanmadığını ve hedeflere ulaşmaya uygun olup olmadığını belirlemek için yapılan sistematik ve bağımsız bir inceleme" olarak tanımlamaktadır (https://www.iso.org/standard/17940.html., 2023)

Bulut teknolojilerinin güvenlik denetiminin zorlukları temel olarak bu sistemlerin karmaşıklığından, kamu ve özel bulutlar arasındaki farklardan, bulut ile kuruluşun sistemleri arasındaki çevre kavramının ortadan kalkmasından kaynaklanmaktadır. Çoğu buluta özgü standartta sağlanan üst düzey öneriler ile mevcut bulut altyapılarında halihazırda var olan düşük düzeyli günlük kayıt bilgileri arasında önemli farklılıklar vardır. Uygulamada, Bulut Hizmeti Tüketicileri (BHT), yöneticileri, tarafından yalnızca sınırlı denetim biçimleri gerçekleştirilebilmekte ve birçok önemli sınırlamaya sahip birkaç uyumluluk aracı bulunmaktadır (Majumdar vd., 2019: 11)

Ulaşılan sonuçlar, bulut teknolojileriyle ilişkili risklerin (güvenlik, gizlilik ve veri bütünlüğü, iş sürekliliği planı, süreç ve sistemlerin güvenilirliği, yeni iş süreçlerinin etkinliği/verimliliği, yasal düzenlemelere uyum) anlaşılması ve ele alınması için yararlı bilgiler sağlamaktadır (https://www.ucop.edu.eu, 2023)

Günümüzde kullanılan denetim metodolojileri ve güvenlik yöntemleri bulut hizmetlerine tam olarak uygulanamamaktadır. Bu durum ise bulutun yaygınlaşmasına yol açan özelliklerin geleneksel teknolojilerden tamamen farklı olmasından kaynaklanmaktadır. Böylelikle kaynakların sanallaştırılması, paylaşılan/ortak sorumluluk kavramının kullanılması ve hizmet sağlayıcının sorumluluğunda olan ekipmanların denetlenememesi, bulutta denetim sürecinin yeni yöntem ve süreçleri gerektirmesine neden olmaktadır. Genel bulut mimarilerinde istemci tarafından gerçekleştirilen güvenlik denetiminin "bulutta denetim" anlamına geldiğini, "bulut denetiminin" ise yalnızca özel bulutlar için yapılabileceğini belirtmek önemlidir. Seçilen bulut hizmetine bağlı olarak, güvenlik denetimi süreci, paylaşılan sorumluluk ilkesine uygun bir biçimde aşağıda Tablo 1'de ifade edilen bileşenlerden meydana gelmektedir (https://www.aws.training, 2023)

Tablo 1. Paylaşılan Sorumluluk Modeli

	IaaS (Yazılım Hizmeti)	PaaS (Platform/Süreç Hizmeti)	SaaS (Altyapı Hizmeti)
Bulut Hizmeti Tüketicileri	İnsanlar Veri Uygulamalar İşletim Sistemi Sanal Ağlar	İnsanlar Veri Uygulamalar	İnsanlar Veri
Bulut Hizmeti Sağlayıcıları	Hipervizörler Sunucular Depolama Fiziksel Ağlar	İşletim Sistemi Sanal Ağlar Hipervizörler Sunucular Depolama Fiziksel Ağlar	Uygulamalar İşletim Sistemi Sanal Ağlar Hipervizörler Sunucular Depolama Fiziksel Ağlar

Kaynak: (Bruma, 2021)

Bulut Hizmeti Tüketicileri (BHT) perspektifinden denetlenecek SaaS (Platform Hizmeti) modeli, en basit model olarak karşılanmaktadır. Çünkü güvenlik konusunda sorumluluk yalnızca kişilere ve verilere aittir. Aynı zamanda sadece kişileri ve verileri denetleyen BHT'nin, diğer bileşenler üzerinde hiçbir sorumluluğu olmaması ve güvenlik denetimi yapamamasından dolayı BHS'nin denetim raporuna güvenmesi gerekmektedir.

Bulut denetim süreci, güvenlik hedeflerine ve gereksinimlerine göre, bir üçüncü taraf denetçi desteği olsun ya da olmasın kamu, özel, iç veya dış denetim olarak nasıl tanımlandığına göre sınıflandırılabilmektedir (Kolhar vd., 2017):

a) İç Denetim: İç denetim mekanizması, Bulut Hizmeti Sağlayıcısı (BHS) tarafından sunulan hizmetlerin güvenlik ve uyumluluk risklerinin yönetilmesine ve değerlendirilmesine yardımcı olmaktır. Tüm süreç, bulut yönetiminde yer alan diğer kuruluşların desteği olmaksızın, yalnızca kuruluş tarafından, kendi yöntem ve mekanizmaları aracılığıyla gerçekleştirilmektedir. Kuruluşun yönetimi tarafından tüm bilgi güvenliği risklerinin tanımlanması kilit role sahiptir.

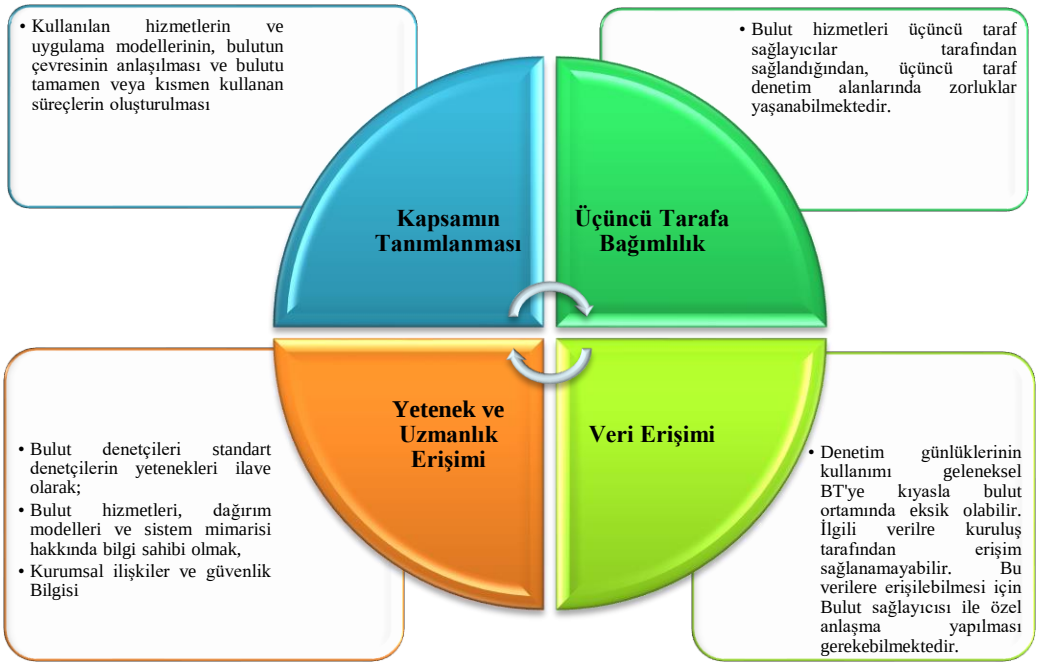
İç denetim açısından bakıldığında, bulut yığınının hangi bölümünün denetleneceğinin belirlenmesinde, hizmetlerin ve altyapının sürekli olarak değiştiği ve geliştiği bir sistemin kontrolleri biçiminde başka sorunlar ortaya çıkabilmektedir. Şekil 1, kapsamın tanımlanması, üçüncü tarafa bağımlılık, beceri ve uzmanlık erişimi ve zamanında veri erişim gibi iç denetimin karşılaştığı temel zorlukları göstermektedir (KPMG, 2023).

b) Bulut Sağlayıcı Denetimi: Denetim faaliyetleri, Bulut Hizmet Sağlayıcısı tarafından gerçekleştirilmektedir. Giants BHS (Google Cloud, Azure, IBM gibi) uluslararası standartlara (Cloud Security Alliance Control Matrix, ISO 27001, SOC 2 vb.) uygunluğu belgeleyen belirli denetim raporları sunmakta ve web siteleri üzerinden erişim sağlanabilmektedir.

c) Özel/Kamu Denetimi: Kurumdan bağımsız kuruluşlar tarafından denetim faaliyetleri gerçekleştirilmektedir. İç denetime veya BHS'ye kıyasla objektif sonuçlar elde edilebilmektedir (Ogigau-Neamțiu, 2018). Güvenlik denetimi sağlayan en büyük şirketlerden biri aşağıdaki yaklaşımı kullanan Deloitte (2023)'dir:

- Mantıksal ve fiziksel güvenlik kontrollerinin test edilmesi
- BT operasyonlarının test edilmesi
- Felaket kurtarma prosedürlerinin test edilmesi
- İş sürekliliğinin test edilmesi
- Veri bütünlüğü değerlendirmesi
- Kritik sistem platformları, ağ ve fiziksel bileşenler, ilgili iş süreçlerini destekleyen BT altyapısı üzerindeki kontrollerin değerlendirilmesi

- BT stratejisi ön izlemesi
- BT organizasyonunun gözden geçirilmesi
- BT süreçlerinin incelenmesi (yardım masası, hizmet yönetimi, uygulama yönetimi ve gözetimi).



Şekil 1. İç Denetimde Karşılaşılan Zorluklar

Kaynak: (KPMG, 2023)

Daha önce ifade edilen üç denetim yönteminden hangisinin kullanıldığına bakılmaksızın, bir denetim sürecinden geçtikten sonra BHS ve BHT için bir dizi öneri sunulabilmektedir (Bruma, 2021: 265):

Bulut Hizmeti Tüketicisi Açısından

• Müşterinin denetim sonuçlarının, özellikle değerlendirmelerin kapsamından bahsedilmesi, hangi hizmetlerin belirli yasa ve yönetmeliklerin kapsamına girebileceği ve müşterinin sorumluluklarının açıkça belirlenmesi,

• Uygunluk sertifikalarının muhafaza edilmesi ve durumundaki herhangi bir değişikliğin bildirilmesi,

• Müşterilere kendileri tarafından toplanamayan gerekli denetim çıktılarının sağlanması önerilmektedir.

Bulut Hizmeti Sağlayıcısı Açısından

• Bulutta dağıtmadan, taşımadan veya geliştirmeden önce uyumluluk yükümlülüklerinin anlaşılması,

• Özellikle müşterinin denetim alanını yönetmek için denetimler ve doğrudan geçiş sertifikaları kullanılacaksa, bulut bilişim deneyimi olan denetçilerin seçilmesi önerilmektedir.

Bulut denetimi için mevcut yöntemler; geriye dönük durdur ve kontrol et denetimi ve proaktif denetim biçiminde üç kategoriye ayrılmaktadır (Ou vd., 2019):

Geriye dönük ve Durdur ve Kontrol Et Denetimi: Denetim sürecini yürütmenin geleneksel yöntemleri olarak ifade edilebilmektedir. *Geriye dönük denetim*, güvenlik önlemleri ve güncellemeleri kullanılarak izinsiz girişlerin ve bilinen güvenlik açıklarının tespit edilmesine dayanmaktadır. İlgili

sistem, önlemlerin kullanımının sonucunu görmek için giriş parametrelerinin eylemine tabidir (https://people.csail.mit.edu.eu, 2023). Ağ bağlantılarının denetlenmesi için kullanılan Microsoft'un SecGuru'su, IBM'in (güvenlik bilgileri ve olay yönetimi) entegre modülleri ve Amazon'un müşterileri bağlamında denetim faaliyetleri için kullanılabilecek çeşitli web API'leri dahil olmak üzere büyük bulut teknolojisi şirketleri tarafından geliştirilen birden fazla güvenlik çözümleri bulunmaktadır (Majumdar, 2018). Ayrıca, güvenlik denetimi sürecinde kullanılabilecek çeşitli açık kaynaklı çözümler de mevcuttur, Facebook tarafından oluşturulan bir işletim sistemi analiz yardımcı programı olan Osquery, SQL sorgularına dayalı olarak uç nokta cihazları için düşük seviyeli analiz yapılmasına olanak tanımaktadır. CloudSploit, bulut altyapısındaki güvenlik risklerinin tespit edilmesini sağlayarak bir dizi yapılandırma hatası ve ilgili güvenlik açıklarını ortaya çıkarmaktadır (https://osquery.readthedocs.io/en/stable/., 2023). Durdur ve kontrol et yöntemi; olayları, engellenmiş halde tutarken önemli doğrulama görevlerini yerine getirmektedir (Majumdar, 2019).

Proaktif Denetim: Güvenlik denetiminin yürütülmesinde proaktif yaklaşım, 1. maddede belirtilen geleneksel denetim yöntemleri ile olay yönetimi faaliyetlerinin birleştirilmesinden oluşmaktadır (Majumdar, 2018).

IV. BULUT UYGULAMALARINDA BİLGİ GÜVENLİĞİ DENETİMİ SÜRECİ

İç denetimden karşılaşılan Şekil 1'de belirtilen zorluklar dikkate alındığında bilgi güvenliği denetimine ilişkin denetim süreci aşağıda yer alan i) denetimin planlanması, ii) bulut denetim standartları ve çerçeveleri, iii) görevler ayrılığı, iv) denetimin yürütülmesi ve v) denetimin tamamlanması ve raporlanması gibi kritik adımlardan çalışmanın teması bağlamında dikkate alınmıştır.

IV.I. Denetimin Planlanması

Yönetim yapılarına, bilgi varlıklarına zarar verebilecek süreç ve faaliyetlerin iyileştirilmesi için faydalı geri bildirimler sağlayan bir denetim sürecinin yürütülebilmesi için, kuruluşların kullanılan veri türüne özgü denetim politikalarını hayata geçirmeleri gerekmektedir. Bir denetim faaliyetinin planlanması, kuruluşun özelliklerine bağlı olarak gerekli aşamaların oluşturulmasını kapsamaktadır. Planlama genellikle denetim hedeflerinin ve amacının belirlenmesinden oluşur:

- Denetimin Hedefleri: Bu sürecin planlama aşaması, denetçilerin kurum ve yürütülen süreçler hakkında genel bir bakış açısı oluşturmasını içermektedir. Politikaları, belirli iç düzenlemeleri ve kurumun çalışma şeklini anlamak için denetlenen tüm bölümlerden bilgi toplanması gerekmektedir (Fazekas, 2018).
- Denetimin Kapsamı: Denetimin amacının tanımlanması, sürece dahil olan tüm bileşenlerin - *personel, sistemler, süreçler* – açıklığa kavuşturulması ile anlam kazanmaktadır. Kaynakları tahsis etmek için sanallaştırmanın ağırlıklı olarak kullanılması denetim sürecini karmaşık hale getirebilmektedir. Çünkü kaynakların soyut hale dönüştürülmesi denetim amacıyla tüm varlıkların tanımlanmasını zorlaştırmaktadır. Bu sorunu çözmek için bazı BHS'ler tüketicilere, altyapılarının uyumluluk standartlarını karşılayıp karşılamadığını teyit edebilecek üçüncü taraf şirketlerden denetim raporları sağlamaktadır (ISC/CCSP, 2023).

ISACA, denetimin planlanması ve kapsamının belirlenmesi, bulutun yönetilmesi ve bulutta faaliyet gösterilmesi olmak üzere 3 aşamaya dayanan bir denetim / güvence programı önermektedir. Veri ve bilgi güvenliği, Tablo 2'de belirtilen kontroller yardımıyla analiz edilmektedir.

Tablo 2. ISACA Denetim/Güvence Programı Adımları

Kategori	Açıklama	Adımlar
Olay Müdahalesi, Bildirim ve Düzeltme	Olay bildirimleri, yanıtlar ve iyileştirmeler belgelenir, zamanında yapılır, olay riski ele alınır, gerektiği şekilde üst kademeye iletilir ve resmi olarak kapatılır.	• Olay Müdahalesi • Servis Sağlayıcı Sorun Takibi • Müşteri Sorunlarının Takibi
Uygulama Güvenliği	Uygulamalar, değişen uygulama mimarilerine dayanabilecek bir risk analizi ve konfigürasyon yönetimi ve provizyon sürecinin tasarımını gerektiren, bulut uygulamalarının doğasında bulunan karşılıklı bağımlılıklar anlayışıyla geliştirilir.	• Uygulama Güvenliği Mimarisi • Yapılandırma Yönetimi ve Sağlama • Uyma • Araçlar ve Hizmetler • Uygulama İşlevselliği
Veri Güvenliği ve Bütünlüğü	Uygulamalar için gizlilik, bütünlük ve kullanılabilirlik sağlar.	• Şifreleme • Anahtar yönetimi
Kimlik ve Erişim Yönetimi	Kimlik süreçleri, verilere ve kaynaklara yalnızca yetkili kullanıcıların erişmesini, kullanıcı etkinliklerinin denetlenip analiz edilebilmesini ve müşterinin erişim yönetimi üzerinde kontrole sahip olmasını sağlar.	• Kimlik Sağlama • Kimlik Doğrulama
Sanallaştırma	Sanallaştırma işletim sistemleri, diğer müşteri ortamlarıyla çapraz çakışmayı önlemek için güçlendirilmiştir.	

Kaynak: (Bruma, 2021: 265)

IV.II. Görevler Ayrılığının Önemi

İş sistemleri açısından temel ve uzun süredir var olan güvenlik kavramlarından biri *"görevlerin ayrılması (veya ayrıştırılması)"* dır. İlgili kavram, birden fazla aktörün yer alması gerekeceğinden dolandırıcılık veya hırsızlık fırsatını azaltmak için bir görevin parçalarını ayırmanın ve daha sonra farklı kişilere ve yerlere devredilmesinin tavsiye edilebilirliğini içermektedir. Ashton'ın (1974) çığır açan davranışsal araştırmasında; denetçileri, yargıları bakımından tutarlılıklarını anlamak için sorgulamıştır.

Yapmış olduğu araştırmada;

- Hem zaman tutma hem de çalışanlara ödeme yapma görevleri bordro hazırlama görevinden yeterince ayrılmış mı?
- Hem bordro hazırlama hem de çalışanlara ödeme yapma görevleri, bordro banka hesabı görevinden yeterince ayrılmış mı?

Bu iki sorudan herhangi birinin cevabının "hayır" olduğuna karar vermenin sonuçları açıktır. Bir bireyin bordroyu kendi yararına manipüle etmesi için bir fırsat ve cazibe ortaya çıkmaktadır. Bordro departmanını ana iş yerinden uzakta konumlandırmak mümkün olsaydı ve bordrodaki hiç kimsenin şirketin geri kalanındaki hiç kimseyi tanımadığından emin olunabilseydi, güven daha da artmış olacaktı. Böyle bir ayrılık sadece dolandırıcılığı zorlaştırmakla kalmaz, aynı zamanda kasıtsız hataların fark edilme olasılığının da daha yüksek olduğu anlamına gelmektedir. Görevlerin ayrılmasına yönelik;

- Gelinas ve Oram (1999), birbirinden ayrılması gereken dört temel işlem belirlemiştir; i) işlemlerin yetkilendirilmesi, ii) işlemlerin yürütülmesi, iii) işlemlerin kaydedilmesi ve iv) işlemlerin tamamlanmasının ardından kaynakların korunması,
- Vaassen ve diğerleri (2009); yetkilendirme, saklama, kayıt, kontrol ve yürütme biçiminde sınıflandırmalar yapmıştır.

Ge ve McVay (2005), Sarbanes-Oxley Yasası'nı (SOX, 2002: 66) takiben yöneticilerin hesaplarının doğruluğunu imzalama sürecinde, hayatlarını tehlikeye attıkları ek açıklamalardan yararlanarak zayıflıklarını kabul eden şirketleri incelemişlerdir. İki yıllık bir zaman aralığına (2002-2004) bakarak, iç kontrol zayıflıklarını itiraf eden 261 firma tespit etmişler ve bunların 45'inin görevler ayrılığının eksikliğini itiraf ettiğini belirtmişlerdir.

IV.III. Denetim Faaliyetlerinin Yürütülmesi

Denetim faaliyetlerinin yürütülmesi kapsamında iç denetçiler BHS tarafından sunulan hizmetlerin; risklerin yönetilmesine ve değerlendirilmesinde, güvenlik ve uyumun sağlanması konusunda kritik role sahiptir. Bütün süreç ilgili kuruluş tarafından kendi yöntem ve mekanizmaları aracılığı ile yerine getirilmektedir. Fakat bu aşamada iç denetim mekanizmasının ve iç denetçilerin sahip olması gereken nitelikler öne çıkmaktadır.

- Bilgi güvenliği risklerinin ortaya koyulması,
- Bulut yığınının hangi alanının ya da bölümünün kim tarafından nasıl denetleneceği,
- Değişen ve gelişen altyapıya ilişkin sistem kontrollerinin nasıl yapılacağı,
- Üçüncü tarafa (BHS) bağımlılık,
- Beceri ve uzmanlık alanına göre denetim çalışmalarının nasıl bölümlendirilerek yürütüleceği,
- Verilere zamanında nasıl erişim sağlanacağı konularında kritik sorular öne çıkmaktadır.

Denetçilerin mesleki yargılarına olan güvenin mevcut değerinin korunması ve artırılmasına yönelik BT becerilerinin üst düzeyde olması gerekliliği konusu iç denetim faaliyetlerinin yerine getirilmesi sürecinde olmazsa olmaz nitelikler arasında yer almaktadır. İlgili süreçte karşılan zorluklar çalışmanın önceki aşamalarında yer alan Şekil 1'de açıklığa kavuşturulmuş olup çözüm önerileri sunulmuştur. Denetim kanıtlarının sağlıklı bir biçimde toplanması, değerlendirilmesi ve isabetli kararlar alınarak sonuca bağlanması konusunda; BHS yönetimi ve işletme yönetimi arasında özel anlaşma yapılması gereksinimi bir diğer kritik adım olarak kabul edilebilmektedir. Bu aşamada ayrıca iç denetçiler tarafından bulut güvenlik denetimi (Bruma, 2021); i) fiziksel güvenlik kontrollerinin test edilmesi, ii) BT operasyonlarının test edilmesi, felaket kurtarma senaryoları ile ilgili prosedürlerin test edilmesi, iii) iş sürekliliği ile veri bütünlüğünün test edilmesi, iv) BT altyapısı, stratejisi, organizasyonu ve süreçlerinin incelenmesi ve test edilmesi ile v) destek hizmetlerinden meydana gelmektedir.

IV.IV. Denetim Faaliyetlerinin Tamamlanması ve Raporlanması

Bulut siber güvenliğinin sağlanmasında kritik üç başarı faktörü öne çıkmaktadır. Bu faktörler; gizlilik, bütünlük ve kullanılabilirlik şeklinde sıralanabilmektedir. İç denetçi tarafından bulutta yer alan yazılım, platform ve altyapı hizmetleri bağlamında (Duncan ve Whittington, 2016);

i) sistemlerin ve bilgilerin,

ii) veri tabanlarının,

iii) işletim sistemlerinin,

iv) uygulamaların,

v) iş sürekliliğinin,

vi) iş süreçlerinin etkinliği ve verimliliğinin; gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak üzere yasa ve standartlara uygun olarak savunma ve güvenlik ekipmanları gibi bileşenler üzerinden makul güvence sağlanmasına hayati rol taşımaktadır. Bu aşamada yaşanan herhangi bir aksaklık ya da erişim sorunu denetim faaliyetlerinin sağlıklı bir biçimde yerine getirilip getirilmemesi ve denetçi görüşünün güvenirliği ve geçerliliği konularında kritik soru işareti oluşturabilecektir.

Geleneksel denetim, siber denetim uygulamalarından farklı olarak özellikle BHS'lerin bulut güvenlik denetimlerinde etkili role sahip olmaları, denetçileri bu aşamada daha farklı alanlarda sorumluluk taşımalarına itmektedir. Dolayısı ile bulut siber güvenliğinin güçlendirilmesinde iç denetim mekanizmasının ve denetçilerin rollerine açıklık getirilmesi önemli görülmekte ve izleyen başlıkta tartışılmaktadır.

V. BULUT SİBER GÜVENLİĞİNİN GÜÇLENDİRİLMESİNDE İÇ DENETİMİN ROLÜ

Siber risk konusunun işletmelere yönelik artan saldırılar ve manipülasyonlar ile birlikte günümüzde teknolojik bir risk olmanın çok ötesine geçmiştir. (Kestane, 2021: 773-796). Siber risklerin kendilerine geniş bir alanda yer edinmeleri beraberinde siber güvenlik sorunlarını meydana getirmiştir. İç denetim mekanizmaları ise karmaşık ve hızlı bir biçimde kendisini gösteren ilgili riskler karşısında kayıtsız kalmaları kaçınılmaz hale gelmiştir. Özellikle iç denetçilerin, denetim komitelerinin ve yönetimin bahsedilen konuya vermiş göstermiş oldukları hassasiyetin denetim süreçlerinin geleceğinin nasıl olacağı konusunda büyün önem taşımaktadır (IIA, 2016: 4).

Uluslararası İç Denetim Enstitüsü tarafından 2016 yılında konuya verilen önem açığa vurulmuştur. Siber güvenlik sorununun bütünleşik olarak belirli bir sistem içerisinde dikkate alınması ve değerlendirilmesine yönelik "*Global Perspektif ve Anlayışlar: Güvenilir Siber Danışmanlık İçin İç Denetim*" başlıklı bir rehber kitapçık yayımlanmıştır. İlgili rehberden, siber güvelik çalışmalarının dışında kalan işletmelerin; ciddi problemler ile karşı karşıya kalabileceği, fikri mülkiyet sahiplikleri ve kişilik haklarının zarara uğrayabileceği hatta varlıklarını devam ettirmelerinin tehlikeye girebileceği anlaşılmaktadır (IIA, 2016). Bahsedilen açıklamalar doğrultusunda siber güvenlik sorununu meydana getiren alanlar üzerinden iç denetim faaliyetlerinin etkileyebileceği kritik dört alan öne çıkmaktadır (IIA, 2017: 10):

- Siber tehditler karşısında ön hazırlık ve olaylara müdahale edilmesi hakkında güvence sağlamak,
- Kuruluşun karşılaşmış olduğu risklerin seviyesi ve risklerin kendisine verilen cevapların seviyesine yönelik yönetim kuruluna bilgilendirmek,
- BT ile kuruluşun diğer birimlerinin birlikte hareket etmesiyle etkin bir önleme ve müdahale mekanizmasının üzerine çalışmak,
- Kuruluş içerisinde risklere karşılık etkili bir iletişimi ve koordinasyon sağlamak şeklindedir.

Enstitü'nün yapmış olduğu açıklamalar incelendiğinde; kuruluşların siber riskler konusunda hazırlıklı ve bilinçli olmaları gerektiği anlaşılmaktadır. Kuruluşlar tarafından ilgili kavram bilinmesine rağmen yetkisiz erişim, kullanıcı/kimlik doğrulama ya da çalma gibi olayların hali hazırda artış eğilimi göstermesinden dolayı olması gereken hassasiyetin gösterilmediği anlaşılmaktadır. Özellikle bu yönde kuruluşların aksiyon alması ise iç denetim fonksiyonu aracılığı ile mümkün olabilecektir. Çünkü kuruluşlarının faaliyetlerinin fiziksel işlemlerden soyut işlemlere dönüşmesi dolaylı olarak iç denetim faaliyetlerinin yapısını, içeriğini ve yönünü de etkilemektedir. Ayrıca siber güvenlik kaynaklı ortaya çıkan açıklar iç denetim fonksiyonunun çalışma alanını genişlemesine yol açmış olup siber risk odaklı faaliyetlerin yeniden yapılandırılması gereksinimi ortaya çıkmıştır. Kuruluşun karşılaşabileceği bütün riskleri içerecek biçimde iç denetim prosedürlerinin hazırlanarak iç kontroller ile de uyumlu olacak şekilde güvence sağlaması beklenmektedir.

Günümüz itibari ile iç denetimin savunma odaklı kontrollerin işleyişini ve etkinliği değerlendirmekte olduğu açıktır (Kurnaz ve Dindaroğlu, 2015). Buna karşılık siber güvenlik açıkları karşısında BT kontrollerinin etkin bir çözüm sunmadığı bilinmektedir. Risklerin izlenmesinden suiistimallerin tespit edilmesine, onarıcı faaliyetlerden ek kontrol anahtarlarına dek birçok mekanizmanın oluşturulması gerekmektedir (IIA, 2016). İç denetim fonksiyonun, kuruluşun yönetim kurulu ile koordineli bir biçimde çalışması suretiyle siber güvenlik çalışmalarında ortak bir hareket alanı sağlanmış olabilecektir. Ayrıca olayların doğru analiz edilmesi ve öngörülebilir güvenlik planlarının hayata geçirilebilmesi bakımın bahsedilen husus kritik öneme sahiptir (IIA, 2018: 6-9).

Bahsedilen siber güvelik ve iç denetim ilişkisinin ayrılmaz bir birlikteliğe dönüştüğü bu çağda siber alanın teknolojik evriminin son göstergesi olarak bulut kavramı gün ışığına çıkmıştır. Siber alan içerisinde belirli bir alanı temsil eden bulutların uygulama sahasındaki yeri genişlemiş ve yeni bir risk alanı daha ortaya çıkmıştır. Bulut siber güvenliği olarak geçen ilgili alan kuruluşlarının faaliyetlerinin fiziksel den soyuta dönüştüğün en önemli somut göstergesi olarak karşılanmaktadır. Denetim dünyasında ilgili konuya ilişkin hali hazırda bir görüş birliği oluşmasa da ilgili uygulamaların denetiminin kaçınılmaz olduğu bir gerçektir. Bulut güvenlik denetimi olgun bir alan olarak kabul görmese de

muhasebe profesyonellerini konfor alanlarından kaldırarak yeni bir adım atmaları yönünde iteceği açıktır.

Uluslararası İç Denetim Enstitüsü'nün siber güvenlik üzerine yapmış olduğu yoğun çalışmaları, ISACA, ENISA ve denetim kuruluşlarının desteklediği çalışmanın daha önceki bölümlerinde belirtilmiştir. Bulut siber güvenliği üzerine Deloitte'un çalışmalarının önemli bir payının olduğunu belirtmekte yarar görülmektedir. Gerçekleştirilen çalışmalar günümüzde istenilen düzeye ulaşmamış olsa da bu konu üzerinde daha çok yol kat edileceği açıktır.

Muhasebe dünyasında denetçilerin teknik bir alana yönelmesi ile bilgisayar geçmişi olanların denetim faaliyetleri içerisinde kendilerini bulmaları ilgili alanda kritik açıklar ve zayıflıklar meydana getirmektedir. Söz konusu açıklık ve zayıflıkların giderilmesinde ise iç denetim birinci derecede sorumluluk sahibidir. Bu aşamada bulut denetim hizmetlerinin sağlanmasında muhasebe uzmanları ve güvenlik uzmanları gibi iki disiplinin bir araya gelmesi, iki farklı profesyonel zihin setiyle mücadele edilmesi gerektiği anlamına gelmektedir. Farklı disiplinlerin bir araya gelmesi sonucunda siber alan, siber güvenlik, bulutlar, yazılım sistemleri, bulut uygulamalarının güvenliği, süreçlerini takiben denetim dünyasına BT uzmanlarından sonra BHS'lerin giriş yapması ile "denetim izi" kavramı ortaya çıkarmıştır. Söz konusu kavramın neyi kastettiği bir sorun haline gelmiş ve tartışmalara yol açmıştır.

Oxford İngilizce Sözlüğünde (OED, 1989) denetim izi için iki faydalı tanım yer almaktadır: *"a) Muhasebe: bir muhasebe kaydındaki herhangi bir kalemin altında yatan ayrıntılı işlemleri doğrulamanın bir yolu; b) Bilgi İşlem: belirli bir kaynak veri kümesine uygulanan bilgi işlem süreçlerinin, işlemlerinin her aşamasını gösteren ve orijinal verilerin yeniden oluşturulmasına izin veren bir kaydı; bir veri tabanının veya bir dosyanın tabi tutulduğu işlemlerin kaydı"*. Görüldüğü üzere, veri tabanı ve dosya arasında tam bir ortak anlayış bulunmamaktadır.

Muhasebe dünyasında, bir denetim izinin tam olarak ne anlama geldiğinin ve öneminin anlaşılması bakımından Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) (Guttman and Roback, 2023) bilgi işlem güvenliği bağlamında, bir denetim izinin ne olduğuna dair çok ayrıntılı bir açıklama sunmuştur. Yapılan açıklamanın OED tanımıyla tutarlı olduğu görülmektedir. Örneğin, Bernstein (Bernstein vd., 2009: 333) denetim izinin şunları içerdiğini öne sürmektedir: *olaylar, günlükler ve bunların analizi*, Chaula (2006) ise şunları önermektedir: *ham veriler, analiz notları, ön geliştirme ve analiz bilgileri, süreç notları, vb.* Yapılan tanımlamalardan kastedilen denetim izi; bulut uygulamalarında yer alan günlük işlemler ve analizleri ile muhasebe kayıtlarında yer alan kalemlerin altında yatan ayrıntılı işlemlerinin doğrulanması üzerinden hareket edilmesi anlamına gelmektedir. Bulut güvenlik denetimi uygulamalarında; BT uzmanları, iç denetçiler, BHS'ler, kuruluşların yöneticileri denetim faaliyetlerinin ayrılmaz bir parçası haline gelmiştir. Dolayısı ile iç denetim mekanizmasının BHS yöneticileri ve BT uzmanları ile kuruluşun yöneticileri ile desteklenmesi gerektiği açıktır. Bundan dolayı iç denetim faaliyetlerinin bulut uygulamalar karşısındaki rolünün güçlendirilmesi bu çalışmanın teması kapsamında denetim izi kavramı üzerinden kumanda edilmektedir.

Birçok bulut kullanıcısı uygun denetim izleri oluşturma konusunda titizdir, ancak bazen bulutta çalışan bir sanal makine (SM) kapatıldığında, çok titizlikle topladıkları denetim izi verileri de dahil olmak üzere her şeyin, kaybolmasını önlemek için adımlar atılmadığı sürece, SM kapanır kapanmaz görünmeyeceğini unutmaktadırlar (Ko vd., 2011). Gerçek dünya koşullarında, çoğu veritabanı yazılımı varsayılan ayarlarda yetersiz denetim izi hükmü ile birlikte gönderilmektedir. Anderson (2008) denetim izinin kullanıcılar tarafından düzenlenmek yerine yalnızca okunabilmesi gerektiği açıktır. Kullanıcıları yalnızca okuma erişimiyle kısıtlamak yeterince basit olsa da bu sistem yöneticileri için geçerli olmamaktadır. Nasıl ki denetim izi adli muhasebecilere bir şirketteki hileli davranışların izini sürmek için bir araç sunuyorsa, bulut ortamındaki denetim izi de saldırılara karşı düzgün bir şekilde korunabildiği takdirde, adli bilimcilere izinsiz girişleri ve diğer yanlış davranışları izlemek için önemli bir temel sunmaktadır. Bir saldırı durumunda, sistem değerlerinin bütünlüğünü korunmasının, en kötü senaryoda sistemi sıfırdan yeniden oluşturmanın ya da saldırıya uğrayan sistemi yeniden yapılandırılmasının mümkün olması gerekmektedir.

Bulut kullanıcıları genellikle çalıştırdıkları sanal makinelerin yalnızca kendi kontrolleri altında olacağını varsaymaktadır. Fakat, sanal makineler BHS'lerin donanımı üzerinde çalışmaktadır. BHS'ler aynı zamanda kalıcı ya da geçici sistem yöneticileri de istihdam etmektedir. BHS kendi kalıcı

personelini yüksek düzeyde denetleyebilirken, geçici çalışanların için aynı durum söz konusu olmayabilmektedir (Catteddu ve Hogben, 2009: 2010). Bir bulut kullanıcısı işlerini güvence altına almak için istediği kadar adım atabilmektedir, fakat denklemdeki önemli bir bileşen olan BHS'lerin; tüm bulut süreçlerinin donanımına ve yazılımına sahip oldukları gerçeğinin göz ardı edilmemesi gerekmektedir. Bulut ilişkisinde, güvenliği sağlama arayışında BHS'lerin vazgeçilmez bir ortak olarak kabul edilmesi gerekmektedir (Duncan ve Whittington, 2015a). Aksi durumda BHS'ler bu hedefi paylaşmaya istekli olmadıkça ve paylaşana kadar, teknik çözümler başarısızlığa mahkûm olacaktır.

Bahsedilen değişmeler ve gelişmelerden hareketle farklı disiplinlerin yeteneklerinden yararlanarak iç denetimin bulut siber güvenliği üzerindeki rolüne ilişkin yazaralar tarafından hazırlanan model aşağıda Tablo 3'te sunulmaktadır.

Tablo 3. Bulut Siber Güvenlik Denetimi Modeli

UYGULAMA ADIMLARI	SİBER DENETİM	BULUT SİBER GÜVENLİK DENETİMİ
Adım I	Siber Güvenlik Değerlendirmesi Siber Risk Profilinin Belirlenmesi	***Kapsamın Tanımlanması*** Kullanılan hizmetlerin ve uygulama modellerinin, bulutun çevresinin anlaşılması ve bulutu tamamen veya kısmen kullanan süreçlerin oluşturulması ***Üçüncü Tarafa Bağımlılık*** Bulut hizmetleri üçüncü taraf sağlayıcılar tarafından sağlandığından, siber risk ve güvenlik değerlendirmesinin yapılması
Adım II	Siber BT Kontrolleri (Tasarım)	***Veri Erişimi*** İşletmelerin, denetçilerin ve bulut hizmeti sağlayıcılarının özel anlaşma yapması Denetim günlüklerinin kullanımı ile tasarım sürecinin denetçi tarafından yeniden yapılandırılabilmesi – ön değerlendirme –
Adım III	Siber BT Kontrolleri (İşletim)	***Yetenek ve Uzmanlık Erişimi*** Bulut hizmetleri, dağıtım modelleri ve sistem mimarisi hakkında donanımlı denetçiler tarafından uygulama erişimi ve kontrolü, kanıt değerlemesi yapılması, güvenlik kontrolü
Adım IV	Yılsonu Değerlendirme	***Gizlilik, Bütünlük ve Kullanılabilirliğin Sağlanması*** - *Güvence Sağlanması* - Olay müdahalesi bildirim ve düzeltme Uygulama Güvenliği Veri Güvenliği ve Bütünlüğü Kimlik ve Erişim Yönetimi Sanallaştırma Sürekli Destek

Kaynak: yazarlar tarafından oluşturulmuştur.

Yukarıda Tablo 3'te belirtilen modele bakıldığında iç denetimin faaliyet alanının evrim geçirdiğini görmek mümkündür. İç denetim penceresinden değişen ve gelişen teknoloji karşısında öncelikle siber denetime geçildiği günümüz itibariyle ise bulut siber güvenlik denetimine gelindiği açıktır. Bulut siber güvenlik denetimlerinin nasıl izlenmesi gerektiğine dair fikir sunan modelde; iç denetimin bulutlar üzerinde önemli bir iz bıraktığını belirtmek yararlı olacaktır. Şöyle ki bulut uygulamalarının içerisinde denetim sürecinin doğru ve tutarlı bir biçimde kurgulanarak yerleştirilmesi hayati önem taşımaktadır. Denetim faaliyetlerinin samut adımlarının soyut uygulamaların içerisine yerleştirilmesi nasıl ki denetim izine dönüşüyor ise denetim faaliyetlerinin gelecekte kuruluşların gelişiminde de izinin silinemeyeceğini ortaya koymaktadır.

SONUÇ VE DEĞERLENDİRME

Dünyanın hemen her alanını etkisi altına alan siber güvenlik problemleri kuruluşların varlıkları sürdürmelerinin önünde kilit bir role sahiptir. Faaliyetlerin gerçekleştirilmesinden yaşam biçimlerine kadar dijital dünyaya entegre olan kuruluşlar; hizmet alanlarını genişletirken beraberinde problemlerinden çeşitlenerek artmasına neden olmaktadır. Bu durumdan denetim faaliyetleri de kendisine düşen payı almaktadır. Bu çalışmada siber alan içerisinde belirli bir alanı temsil eden bulut bilgi işlem uygulamalarının güvenliğinin güçlendirilmesinde iç denetimin rolünün belirlenmesi amaçlanmıştır. Uluslararası alanda farklı araştırmacılar tarafından çeşitli çalışmalar yapılmış olsa da Türkiye'de çalışmaların sınırlı olması ve erişim güçlüğü yaşanmasından dolayı bu çalışma teorik perspektiften ele alınmıştır. Siber güvenlik teknolojisinin son göstergesi olan bulut uygulamalarına ilişkin bulut güvenlik denetiminin nasıl yapılabileceği ve iç denetimin bu süreçte ki rolünün nasıl olabileceği konusu merak uyandırmış ve bu çalışmanın özgün değerini oluşturmuştur. Çalışmada siber güvenlik, bulut siber güvenliği ve iç denetimin kesişmesinden ortaya çıkan anahtar göstergeler aşağıdaki gibi sıralanabilmektedir:

- Dünya genelinde bulut uygulamalara ve siber güvenliğe ilişkin düzenlemelerin daha çok özel kuruluş tarafından yapılmış olması artı bir değer oluşturur iken buna karşılık ülkelerin otoriteleri tarafından düzenlemelerin çok sınırlı olduğu,
- Yapılan düzenlemelerin proaktif olmaktan öte reaktif niteliklere sahip olmasından dolayı uygulamada etkinliğin zayıf olduğu,
- Kalite standartlarının teknoloji gelişimine bağlı olarak güncelleme yapılması konusunda geride kalındığı,
- Güvenlik sorunlarının giderilmesinde interaktif denetim prosedürlerinin yetersiz olduğu,
- Bulut uygulamalarının geçici bir doğaya sahip olmasından dolayı suiistimallere daha çok maruz kalınabileceği, şeffaflık, hesap verebilirlik, objektiflik ve tam açıklama esaslarının sekteye uğrayabileceği,
- Denetçilerin mevcut yeteneklerinin BT denetimi, siber denetim, bulut siber güvenliği konularında geliştirilmesi gerekliliği,
- Siber suçların önüne geçilmesi konusunda caydırıcı politika ve prosedürlerin hazırlanması ve yürürlüğe koyulması gerektiği,
- Bulut Hizmeti Sağlayıcılarının altyapı, süreç ve hizmet üçgeninde mütekabiliyet kriterlerini dikkate alarak uygulamada aktif görev almalarının gerektiği,
- İç denetimin dijital dünyada ki rolünün gizlilik, bütünlük ve kullanılabilirlik temelinde yeniden yapılandırılması gerektiği,
- Bulut bilgi işlem uygulamalarında güvenliğin güçlendirilmesi bakımından iç denetim tarafından teknolojik kontrol anahtarlarının geliştirilmesi gerektiği,
- Siber saldırıların önlenmesi konusunda özellikle kullanılan bulut uygulamalarının doğasına uygun risk yönetimi süreçlerinin kurgulanması gerektiği, sonuçlarına ulaşılmıştır.

Araştırma neticesinde tespit edilen anahtar göstergelere ilişkin öncelikle mesleki kuruluşların aksiyon alması büyük değişimlerin tetikleyici silahı olarak görülebilmektedir. Denetim mesleği dünya genelinde kabul gören ve yenilikler karşısında sürekli kendisini yenileyen dinamik bir yapıya sahip olmasından dolayı ülkeleri yöneten otoritelere daha geniş perspektiften danışmanlık rolüne sahiptir. Yasal ve kanuni düzenlemelerin teknoloji gelişimine paralel olarak güncellenmesi ekonomik hayatın sağlıklı bir zeminde yol almasına olanak tanıyacaktır. Bulut uygulamalar konusunda Uluslararası İç Denetim Enstitüsü'nün yapmış olduğu çalışmalar ISACA gibi kuruluşların ilgili çalışmaları desteklemesi gurur vermekte fakat yeterli görülmemektedir. Bu noktada uluslararası mesleki örgütlerin bulut uygulamaların güvenliği konusunda ortak bir rehber hazırlaması denetim mesleğinin erozyona

uğramasının önünde mihenk taşı olacaktır. Diğer taraftan eğitim kuruluşlarının konu ile yakından ilgilenmeleri ve müfredatlarını bu yönde güncellemeleri büyük önem taşımaktadır.

Gelecekte denetim mesleğinde; teknik ve teknolojik yönden donanımlı denetçilerin var olması gerektiği kaçınılamaz bir gerçektir. Türkiye'de mesleki kuruluşların, düzenleyici ve denetleyici otoritenin konu üzerinde önemle çalışması önerilmektedir. Fiziksel dünyadan dijital dünyaya iki taraflı bir yaşam alanının kesişiminde yer alan ve denge kuramayan kuruluşların, çalışma alanlarının ve mesleklerin ciddi tehlikeler ile karşı karşıya kalacağı düşünülmektedir. Denetim faaliyetlerinin dünyanın bir bölgesinde geçmişe dönük savunmacı yaklaşım il sürdürülmesi karşısında diğer bölgede bulut uygulamalar içerisinde ize dönüşmesi gelişim açısından aradaki farkı ortaya koymaktadır. Dolayısıyla kurumsal yönetim anlayışının yeniden yapılandırılması ve iç denetim mekanizmasının yerinin ve öneminin belirlenmesi kritik bir ihtiyaç olarak karşılanmaktadır. Bu çalışma ile bulut siber güvenliğinin güçlendirilmesinde iç denetim mekanizmasının mevcut durumuna ve gelecekteki rolü ile denetçilerin niteliklerine ilişkin bir ışık tutulması hedeflenmiştir. Kurgulanan modelin farklı araştırmacılar tarafından daha zengin araştırmalar yapılarak geliştirilmesi beklenmektedir.

KAYNAKÇA

Albersmeier, F., H. Schulze, G. Jahn, & Spiller, A. (2009). The reliability of third-party certification in the food chain: from checklists to risk-oriented auditing, *Food Control*, 20(10), 927–935.

Alliance, C., (2011). Security guidance for critical areas of focus in cloud computing V3.0, Cloud Security Alliance, https://cloudsecurityalliance.org/guidance/ csaguide.v3.0.pdf, (Erişim tarihi: 10.08.2023)

Alliance, C. S. (2016). The Treacherous Twelve - Cloud Computing Top Threats İn 2016. https://cloudsecurityalliance.org/press-releases/2016/02/29/cloud-security-alliance-releases-the-treacherous-twelve-cloud-computing-top-threats-in-2016/ (Erişim Tarihi: 27.07.2023)

Anderson, R. J. (2008). *Security Engineering: A Guide to Building Dependable Distributed Systems*, C. A. Long, Ed. Wiley USA.

Archer, J. & Boehm, A. (2009). Security guidance for critical areas of focus in cloud computing, *Cloud Security Alliance*, 2, 1-76.

Arjoon, S. (2012). Corporate Governance: An Ethical Perspective. *J. Bus. Ethics*, 61(4), 343–352.

Ashton, R. H. (1974). An experimental study of internal control judgements. *J. Account. Research*, pp. 143-157.

Australia Government. (2013). *Strong And Secure.* A Strategy For Australias National Security.

Baldwin, A. D. Pym, & Shiu, S. (2013). Enterprise ınformation risk management: dealing with cloud computing, *Abdn.Ac. Uk*, 257-291.

Behl, A. & Behl, K. (2012). An analysis of cloud computing security issues, *İn Information And Communication Technologies (Wıct),* 2012 World Congress On, 109-114.

Bernstein, D., E. Ludvigson, K. Sankar, S. Diamond, & Morrow, M. (2009). Blueprint For The İntercloud - Protocols And Formats For Cloud Computing İnteroperability. *İn Proc. 2009 4th Int. Conf. Internet Web Appl. Serv*. Icıw,pp. 328–336.

Bernstein, D., E. Ludvigson, K. Sankar, S. Diamond, & Morrow, M. (2009). Blueprint for the intercloud - Protocols and formats for cloud computing interoperability. *In Proc. 2009 4th Int. Conf. Internet Web Appl. Serv.* ICIW 2009, 328–336.

Bruma, L. M. (2021). Cloud security audit – issues and challenges. *The 16th International Conference on Computer Science & Education (ICCSE 2021) August 18-20*, 263-266.

Canada Government (2010). *Canadas cyber security strategy.* Canada: For A Stronger and More Prosperous.

Catteddu, D. (2010). Cloud computing: bene_ts, risks and recommendations for information security. *Springer*, 17(17), 1-15.

Catteddu, D. & Hogben, G. (2009). Cloud computing: benefits, risks and recommendations for ınformation security, *Computing*, 72(1), 2009-2013.

Chapin, F.S., G. P. Kofinas & Folke, C. (2009). Principles of Ecosystem Stewardship: Resilience-Based Natural Resource Management in a Changing World. *Springer*, 1-14.

Chaula, J. A. (2006). A socio-technical analysis of ınformation systems security assurance: a case study for effective assurance. Ph.D. dissertation, 2006.

http://scholar.google.com/scholar?hl=en\&btnG=Search\&q=intitle:A+Socio-Technical+Analysis+of+Information+Systems+Security+Assurance+A+Case+Study+for+Effective+Assurance\#1 (Erişim Tarihi: 02.08.2023)

Chen, Z. & Yoon, J. (2010). It auditing to assure a secure cloud computing. *İn Proc. - 2010 6th World Congr. Serv. Serv*., 253–259.

Chou, D.C. (2015). Cloud computing risk and audit issues. *Computer Standards & Interfaces,* 42, pp. 137-142,

Clavister, C. (2008). Security İn The Cloud, White Paper. https://www.google.com/search?q=Clavister%2C+C.+(2008)%2C+Security+%C4%B0n+The+Cloud%2C+White+Paper.&rlz=1C1NHXL_trTR762TR762&oq=Clavister%2C+C.+(2008)%2C+Security+%C4%B0n+The+Cloud%2C+White+Paper.&aqs=chrome..69i57j0i546l3.918j0j4&sourceid=chrome&ie=UTF-8 (Erişim Tarihi: 16.07.2023)

Claycomb W. R., & Nicoll, A. (2012). Insider threats to cloud computing: directions for newresearch challenges, *İn 2012 Ieee 36th Annual Computer Software And Applications Conference,* 387-394.

Coucil, C. S. C. (2015). *Coucil, Security For Cloud Computing Ten Steps To Ensure Success Version 2.0*, Report, March, 2015.

Craigen, D. Diakun-Thibault, N. & Purse, R.. (2014). Definining Cybersecurity, *Technology Innovation Management Review*, 4, 1-16.

Deloitte (2023), https://www2.deloitte.com/rs/en/pages/technology/solutions/it_audit_and_information_system_security_deloitte_serbia_technology_services_solutions.html. (Erişim Tarihi: 21.07.2023)

Doelitzscher, F., M. Knahl, C. Reich, & Clarke, N. (2013). Anomaly Detection In Iaas Clouds, *İn Proc. Int. Conf. Cloud Comput. Technol. Sci. Cloudcom*, 1, 387–394.

Duncan, B. & Whittington, M. (2014). Compliance with standards, assurance and audit: does this equal security? *in Proc. 7th Int. Conf. Secur. Inf. Networks. Glasgow: ACM*, 77–84.

Duncan, B. & Whittington, M. (2015a), Enhancing cloud security and privacy: broadening the service level agreement, *in 14th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. (IEEE Trust.*, Helsinki, Finland, 1088–1093.

Duncan, B. & Whittington, M. (2015b). Reflecting on whether checklists can tick the box for cloud security, *in Proc. Int. Conf. Cloud Comput. Technol. Sci. CloudCom, vol. 2015-Febru, no. February. Singapore*: *IEEE*, 805–810.

Duncan, B. & M. Whittington, (2015c). The ımportance of proper measurement for a cloud security assurance model, *in 2015 IEEE 7th Int. Conf. Cloud Comput. Technol. Sci., Vancouver*, 1–6.

Duncan, B. & Whittington, M. (2015d). Information security in the cloud: should we be using a different approach*?*. *In 2015 IEEE 7th Int. Conf. Cloud Comput. Technol. Sci., Vancouver*, 1–6.

Duncan, B. & Whittington, M. (2015e). Company management approaches stewardship or agency: which promotes better security in cloud ecosystems? In Cloud Comput. 2015. *Nice: IEEE,* 154–159.

Duncan, B. & Whittington, M. (2016a). Enhancing Cloud Security and Privacy: The Power and the Weakness of the Audit Trail, *In Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization. Rome: IEEE*, 125-130.

Duncan, B. & Whittington, M. (2016b). Enhancing cloud security and privacy: the cloud audit problem, *In Cloud Comput. 2016 Seventh Int. Conf. Cloud Comput. GRIDs, Virtualization. Rome: IEEE*, 19-124.

Duncan, B., D. J. Pym, & Whittington, M. (2013), "Developing a Conceptual Framework for Cloud Security Assurance," in Cloud Comput. Technol. Sci. (CloudCom), 2013 IEEE 5th Int. Conf. Bristol: IEEE, 120–125.

ENISA. (2014). Security Standards For Cloud Usage, Report, August 2014.

Farkan, S. Bashir & Haider, S. (2011). Security threats in cloud computing, in ınternet technology and secured transactions (Icıtst), *2011 International Conference For*, 214-219.

Fazekas, G. (2018). Cloud Computing Auditing, *(IJACSA) International Journal of Advanced Computer Science and Applications*, 19(12), 467-472.

G. Brunette & Mogull, R. (2009). Security guidance for critical areas of focus in cloud computing v2. 1, *Cloud Security Alliance*, 1-76.

Gasser, M. (1988). *Building A Secure Computer System*, New York: Van Nostrand Reinhold Co.

Ge W. & McVay, S. (2005). The disclosure of material weaknesses in internal control after the sarbanes-oxley act, *Account. Horizons*, 19(3), 137–158.

Gelinas U.J. & Oram, A. E. (1999). *Accounting Information Systems (4th edition*). Ohio: South-Western College Publishing, Cincinnati,

Germany Government, (2011). Cyber Security Strategy For Germany.

Gill, A. (2008). Corporate governance as social responsibility: a research agenda, *Berkeley J. Int'l L*., 26(2), 452–478.

Guttman, R. & Roback, E. A. (2023). Computer security, *NIST*, Tech. Rep. 800, 2011. http://books.google.com/books?id= (Erişim Tarihi 16.08.2023)

Holland Government. (2013). National Cyber Security Strategy 2: From Awareness To Capability.

https://github.com/aquasecurity/cloudsploit. (Erişim Tarihi: 28.07.2023)

https://global.theiia.org/translations/PublicDocuments/GPI-2018-Top-Risks-Faced-by-CAES-Turkish.pdf (Erişim Tarihi: 17.01.2023)

https://osquery.readthedocs.io/en/stable/. (Erişim Tarihi: 28.07.2023)

https://people.csail.mit.edu/nickolai/papers/wang-rad.pdf. (Erişim Tarihi: 28.07.2023)

https://www.aws.training, Erişim Tarihi: (21.06.2023)

https://www.iso.org/standard/17940.html. (Erişim Tarihi: 20.06.2023)

https://www.ucop.edu/ethics-complianceaudit-services/_files/webinars/10-14-16-cloudcomputing/cloudcomputing.pdf. (Erişim Tarihi: 21.06.2023)

Humphreys, E. (2008). Information security management standards: Compliance, governance and risk management, *Inf. Secur. Tech. Rep.*, 13(4), 247–255.

Huse, M. (2005). Accountability and creating accountability: a framework for exploring behavioural perspectives of corporate governance, *Br. J. Manag.*, 16(1), 65–79.

IIA, (2016). Global Perspektifler ve Anlayışlar: Güvenilir Bir Siber Danışman Olarak İç Denetim. *The Institute of Internal Auditors.* https://global.theiia.org/translations/PublicDocuments/GPI-Emerging-Trends-Turkish.pdf (Erişim Tarihi: 08.02.2023)

IIA, (2017). Küresel Bakış Açıları ve Anlayışlar Yapay Zekâ – İç Denetim Mesleğine İlişkin Dikkate Alınması Gerekenler. *The Institute of Internal Auditors.* https://global.theiia.org/translations/PublicDocuments/GPI-Artificial-Intelligence-Part-I-Turkish.pdf (Erişim Tarihi: 11.01.2023)

IIA, (2018). Global Bakış Açıları ve Anlayışlar: 2018 Global Risk Raporu-İç Denetim Yöneticilerinin Karşılaştığı En Büyük Riskler. The Institute Of Internal Auditing.

Ioannidis, C., D. Pym, & Williams, J. (2013). Sustainability in Information Stewardship: Time Preferences, Externalities and Social Co-Ordination, *In Weis*, pp. 1–24.

ISACA, (2009). An Introduction to the Business Model for Information Security, Tech. Rep., 2009.

ISC/CCSP (2023). Certified Cloud Security Professional Official Study Guide.

ISECT, (2011). Information Security Frameworks from "Audit" to "Zachman"," *Tech. Rep.* March.

ITU, (2023), Overview Of Cybersecurity (ITU-T X.1205), 04/2023.

Kestane, A. (2021). Siber güvenliğin etkinleştirilmesinde sürekli süreç denetimi modeli, *Muhasebe Bilim Dünyası Dergisi Aralık,* 23(4), 773-796.

Ko, R. K. L., P. Jagadpramana, M. Mowbray, S. Pearson, M. Kirchberg, Q. Liang, & B. S. Lee, (2011). TrustCloud: A framework for accountability and trust in cloud computing, *Proc. - 2011 IEEE World Congr. Serv. Serv.*, 584–588.

Kolhar, M., A. Alameen, B. Dhupia, S. Rubab & Gulam, M. (2017). *Cloud Computing Data Auditing Algorithm*, England: Notion Press.

Kolk, A. (2008). Sustainability, accountability and corporate governance: Exploring multinationals' reporting practices. *Bus. Strateg. Environ*., 17(1), 1–15.

KPMG (2023). https://home.kpmg/be/en/home/insights/2020/11/ta-cloudcomputing-and-the-internal-audit-function.html. (Erişim Tarihi: 21.06.2023)

Kumar, R. Nandha,T. Sathiya, H. C. M. ,Sayed S.A. , Ankit K., Ghalib H. A. & Henry K. A. (2022). Secure data deduplication system with cyber security multikey management in cloud storage, *Hindawi Security And Communication Networks*, 1-13.

Kurnaz, N. & Dindaroğlu, A. K. (2015). İç denetim ve bilgi güvenliği ilişkisi: bölgesel bir araştırma, *Bilgi Ekonomisi ve Yönetim Dergisi*, X (1), 52-63.

Kurt, G. & Uçma Uysal, T. (2015). Siber riskler ve coso iç kontrol bütünleşik çerçevesi, *Muhasebe ve Denetime Bakış,* Ekim 2015, ss. 1-10.

Lacity, M. C. (2012). Advanced outsourcing practice: rethinking ito, bpo and cloud services, Palgrave Macmillan. https://scholar.google.com.tr/scholar?q=Lacity,+M.+C.+(2012),+%E2%80%9CAdvanced+Outsourcing+Practice:+Rethinking+%C4%B0to,+Bpo+And+Cloud+Services%E2%80%9D,+Palgrave+Macmillan.&hl=tr&as_sdt=0&as_vis=1&oi=scholart (Erişim Tarihi: 29.07.2023)

Le, Ngoc T. & Hoang, Doan B. (2017). Capabılıty maturıty model and metrıcs framework for cyber cloud securıty, Https://Opus.Lib.Uts.Edu.Au/Bitstream/10453/121301/1/Cscmm-Scpe-01-5-2017.Pdf (Erişim Tarihi: 26.08.2023)

Leavitt, N. (2009). Is Cloud Computing Really Ready For Prime Time?, *Computer (Long. Beach. Calif)* 42, 15–20.

Li K. C., Chen X. & Susilo W. (2019). Foreword I-II. Kuan-Ching, L. Xiaofen, C. Ve Willy, S. (Eds.) Advances İn Cyber Security: Principles, Techniques, And Applications, Springer Nature Singapore Pte Ltd., Singapore.

Lopez, J. M., T. Ruebsamen, & Westhoff, D. (2014). Privacy-friendly cloud audits with somewhat homomorphic and searchable encryption, *İn 14th Int. Conf. Innov. Community Serv. "Technologies Everyone*, I4cs 2014 - Conf. Proc95–103.

Majumdar, S. (2018). Proactive Security Auditing for Clouds, Montreal.

Majumdar, S., T. Madi, Y. Wang, A. Tabiban, M. Oqaily, A. Alimohammadifar, Y. Jarraya, M. Pourzandi, L. Wang & Debbab, M. (2019), *Cloud Security Auditing*, Springer, 1-8.

New Zealand Government, (2015). New Zealand's Cyber Security Strategy.

OED-Oxford English Dictionary (1989). www.oed.com (Erişim Tarihi: 30.07.2023)

Ogigau-Neamțiu, F. (2018). Cercetarı Prıvınd Securızarea Informatıeı Tn Sıstemele Cloud Computıng, Brașov.

Order, T. (2013). Executive Order 13636: Improving Critical Infrastructure, *Cybersecurity*, pp. 1–8.

Ottis, R. & Lorents, P. (2010). Cyberspace: definition and implications, *In Proceedings Of The 5th International Conference On Information Warfare And Security*, 267-270.

Ou, M., L. Wang & Xun, H. (2019). DeaPS: DeepLearning-Based User-Level ProactiveSecurity Auditing for Clouds, *In 019 IEEE Global Communications Conference (GLOBECOM).*

Papanikolaou, N., S. Pearson, M. C. Mont & Ko, R. K. L. (2011), towards greater accountability in cloud computing through natural-language analysis and automated policy enforcement, *Engineering*, 1–4.

Pearson S. & Benameur, A. (2010). Privacy, security and trust ıssues arising from cloud computing, *İn 2010 Ieee Second Int. Conf. Cloud Comput. Technol. Sci., No. December. IEEE*, 693–702.

Prislan, K. & Bernik, I. (2010). Risk management with ıso 27000 standards in ınformation security, *Inf. Secur.*, 58–63.

PWC, (2010). Information Security Breaches Survey 2010 Technical Report, pp. 1–22.

PWC, (2012). UK Information Security Breaches Survey - Technical Report 2012, London, Tech. Rep. April, 2012.: www.pwc. comwww.bis.gov.uk (Erişim Tarihi: 16.07.2023)

PWC, (2024). Bulut Risk ve Yönetişim Hizmetleri, https://www.pwc.com.tr/bulut-risk-ve-yonetisim-hizmetleri (Erişim Tarihi: 25.06.2024)

Rajnovic, D., (2012). Cyberspace What İs İt?, https://www.techopedia.com/definition/2493/cyberspace (Erişim Tarihi: 15.08.2023)

Rissi J. & Sherman, S. (2011). Cloud-based it audit process, *John Wiley & Sons, Inc.*,44, 15–32.

Ruebsamen, T. & C. Reich, (2013). Supporting cloud accountability by collecting evidence using audit agents, *İn Proc. Int. Conf. Cloud Comput. Technol. Sci. Cloudcom*, 1, 185–190.

S. Srinivasamurthy, F. Wayne, & Liu, D. Q. (2013). Security and privacy in cloud computing : a survey security and privacy in cloud computing, *In 2010 Sixth Int. Conf. Semant. Knowl. Grids*, 2, 126–149.

Sang, T., (2013). A log-based approach to make digital forensics easier on cloud computing, *Proc. 2013 3rd Int. Conf. Intell. Syst. Des. Eng. Appl. ISDEA*, 91–94.

Saxena, D., Gupta, I. & Gupta, R. (2023). An Aı-Driven Vm Threat Prediction Model For Multi-Risks Analysis-Based Cloud Cybersecurity, *IEEE Xplore*, 1-13.

Scholar, N.S. & Jeyarah, A. (2021). Recent security challenges in cloud computing, *Computers And Electrical Engineering* 71, 28–42.

Sendi, S. & Cheriet, M. (2014). Cloud computing: a risk assessment model, *2014 IEEE Int. Conf. Cloud Eng.*, 147–152.

Sox, (2002). Sarbanes-Oxley Act of 2002.

Swain, B., P. Agcaoili, M. Pohlman, & Boyle, K. (2010). Cloud Controls Matrix, https://scholar.google.com.tr/scholar?lookup=0&q=Swain,+B.,+P.+Agcaoili,+M.+Pohlman,+and+K.+Boyle,+(2010),+Cloud+Controls+Matrix,+2010&hl=tr&as_sdt=0,5 (Erişim Tarihi: 14.08.2023)

Trend, (2012). 2012 Annual Security Roundup: Evolved Threats in a "PostPC" World," Trend Micro, Tech. Rep.

Vaassen, E., R. Meuwissen, & Schelleman, C. (2009). *Accounting İnformation Systems And İnternal Control.* New York: Wiley Publishing.

Verizon, N. High, T. Crime, I. Reporting, & Service, I.S. (2012). 2012 Data Breach Investigations Report, Verizon, Tech. Rep.

Vouk, M. (2008). Cloud computing ıssues, research and ımplementations,*Itı 2008 - 30th Int. Conf. Inf. Technol. Interfaces*, 16(4), 235–246.

Wang, C., Q. Wang, K. Ren, & Lou, W. (2010). Privacy-preserving publicauditing for data storage security in cloud computing, *İn Ieee Infocom 2010*, 62(2), 362–375.

Wang, L., J. Zhan, W. Shi, Y. Liang, & Yuan, L. (2009). In cloud, do mtc or htc service providers benefit from the economies of scale?, *Proc. 2nd Work. Many-Task Comput. Grids* Supercomput. - Mtags '09, 1–10.

Willingmyre, T. G. (1997). Standards at the Crossroads, *Standard View*, 5(4), 190–194.

Wyatt M. (2017). Cybersecurity Systems: Acquisition, Development, And Maintenance. Domenic, A. (Ed.), The Cyber Risk Handbook: Creating And Measuring Effective Cybersecurity Capabilities. John Wiley & Sons, Inc., New Jersey.

Zio, E. (2009). Reliability Engineering: Old Problems and New Challenges, *Reliab. Eng. Syst. Saf.*, 94(2), 125–141.

Etik Beyanı **:** *Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazarlar beyan eder. Aksi bir durumun tespiti halinde ÖHÜİİBF Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalışmanın yazar(lar)ına aittir.*

Yazar Katkıları **:** Yazarlar eşit katkı sunmuşlardır.

Çıkar Beyanı **:** *Yazarlar arasında çıkar çatışması yoktur.*

Ethics Statement **:** *The authors declare that ethical rules were followed in all preparation processes of this study. If a contrary situation is detected, ÖHÜİİBF Journal has no responsibility and all responsibility belongs to the author(s) of the study.*

Author Contributions **:** *The authors contributed equally.*

Conflict of Interest **:** *There is no conflict of interest between the authors. The institution from which financial support is received (if any) is stated here.*