Üçüncü Sektör Sosyal Ekonomi Dergisi
Third Sector Social Economic Review
54/1 (2019) 478-501
doi: 10.15659/3.sektor-sosyal-ekonomi.19.03.1086

Araştırma Makalesi

Küçük ve Orta Büyüklükteki İşletmelerde Bilgi Güvenliği

Information Security in Small And Medium Size Companies

Murat Sami BAYKIZ	Cihan TANRIÖVEN
İç Denetçi, Gazi Üniversitesi, Bilişim Enstitüsü, Yönetim Bilişim Sistemleri mbaykiz@gmail.com https://orcid.org/0000-0001-9129-3619	Prof. Dr. Ankara Hacı Bayram Veli Üniversitesi, İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü cihantt@gmail.com https://orcid.org/0000-0003-0192-7628

Makale Gönderme Tarihi	Revizyon Tarihi	Kabul Tarihi
04.02.2019	07.03.2019	14.03.2019

Öz

Küçük ve Orta Büyüklükteki İşletmeler (KOBİ) ülke ekonomilerinin lokomotifleridir. KOBİ'lerin esnek yapıları, değişime çabuk adapte olmaları; ülke ekonomilerinin krizleri çabuk atlatmalarını kolaylaştırmaktadır. Rekabet, değişim, küreselleşme gibi etkenler KOBİ'leri bilgi ve iletişim teknolojilerini kullanmayı zorunlu kılmaktadır. Bu teknolojiler sayesinde zaman ve mekân kavramı ortadan kalkmış, bir mobil araç ve ağ sayesinde dünyanın herhangi bir yerinden elektronik finansal hizmet ve ürünlere ulaşmak mümkün hale gelmiştir. Bütün bu gelişmelere paralel olarak; özellikle son yıllarda yaşanan sosyal mühendislik katkılı dolandırıcılık olayları ve çalışan suiistimalleri bilgi güvenliğini ön plana çıkarmıştır. Bilgi teknolojileri konusunda nitelikli yeterli işgücü istihdam etmeyen, bilgi güvenliği riski yalnızca büyük şirketleri etkiler önyargısına sahip KOBİ'ler, teknoloji hırsızları için kolay hedefler haline gelmektedir. Geçmişteki kasa hırsızlarının yerlerini artık klavye hırsızları almıştır. Bilgi güvenliği sağlanamaması sonucu oluşan riskler; itibar riski, yasal risk gibi diğer riskleri de beraberinde getirmektedir. Bu çalışmanın amacı; ellerinde kısıtlı imkânlar bulunan KOBİ'lerin bilgi güvenliği risklerine karşı kullanabilecekleri basit ve yalın bir metodolojinin ortaya çıkarılmasıdır.

Anahtar Kelimeler: *Küçük ve Orta Büyüklükteki İşletmeler, Bilgi Güvenliği, Risk Değerlendirmesi*

Abstract

Small and Medium Enterprises (SMEs) are locomotives of national economies. Flexible structures of SMEs and their quick adaptation to changes make easier for the economies of countries to overcome the crises quickly. Factors such as competition, change and globalization require SMEs to use information and communication technologies. As a result of these technologies, the concept of time and space has disappeared, and it becomes very easy to reach electronic financial services and products from anywhere in the world via a mobile tool and network. In parallel with all these developments; especially in recent years, social engineering added fraud incidents and employee misconceptions highlighted information security. SMEs, which do not employ sufficient qualified labor force in information technology and have prejudge that information security risks only affect large companies, are becoming easy targets for technology thieves. Keyboard thieves have now taken over the place of the thieves of the past. The risks arising as a result of not providing information security bring along with other risks such as reputation risk and legal risk. The purpose of this study is to reveal a simple and plain methodology for SMEs with limited opportunities to use against information security risks.

Key words*: Small and Medium Enterprises, Information Security, Risk Assessment*

Önerilen Atıf /Suggested Citation
Baykız, M.S. , Tanrıöven, C. 2019, Küçük ve Orta Büyüklükteki İşletmelerde Bilgi Güvenliği, *Üçüncü Sektör Sosyal Ekonomi Dergisi*, 54(1), 478-501.

1. Giriş

Özellikle 20. yüzyılın sonlarına doğru bilgi ve iletişim teknolojilerindeki gelişimin hızla iş süreçlerine uygulanması sonucu; işletmelerin iş görme biçimleri değişmiş, bu değişim süreci kimi işletmeler için bir fırsat olurken, kimi işletmeler için risklere, krizlere yol açmıştır.

Büyük şirketler bilgi ve iletişim teknolojilerinden kaynaklanan bilgi güvenliğine ilişkin risklere karşı; bütçe ayırarak, yeterli profesyonel işgücü istihdam ederek gerekli tedbirleri almaya çalışırken, bilgi güvenliğine yatırım yapmayan, maliyetler nedeniyle yeterli sayıda bilgi teknolojileri personeli istihdamından kaçınan KOBİ'ler gerekli tedbirleri alamamakta, suiistimallere ve siber suçlulara karşı kolay hedefler haline gelmektedirler.

Bilgi ve iletişim teknolojisini geliştirmede başı çeken ülkelerde faaliyet gösteren KOBİ'ler dahi risklere maruz kalabilmektedirler. İçlerinde Almanya, Amerika gibi gelişmiş ülkelerin de bulunduğu ülkelerde yapılan bir araştırmada; 2017 yılı içerisinde KOBİ'lerin %47'sinin en az bir kez bilgi güvenliği saldırısına maruz kaldığı tespit edilmiştir (Hiscos, 2018). Yine yapılan başka bir araştırmada; saldırılara maruz kalan KOBİ'lerin %60'ının altı ay içerisinde faaliyetlerini sonlandırdıkları belirtilmektedir (Miller, 2017).

Bilgi güvenliği risklerine karşı alınması gereken tedbirlere ilişkin yapılan araştırmalarda KOBİ'lerin özellikleri genellikle göz ardı edilmektedir. Küresel ekonomik aktivitenin önemli bir bölümünü oluşturan KOBİ'lerin farklı özellikleri nedeniyle, daha büyük kuruluşlar için geliştirilen bilgi güvenliği yönetimine yaklaşımlar KOBİ'ler bağlamında uygulanabilir değildir (Tawileh, Hilton ve McIntosh, 2007).

KOBİ'ler, finansal kısıtlamalar, sınırlı kaynaklar ve yetersiz bilgi birikiminden dolayı bilgi güvenliğini uygun şekilde güvence altına alma araçlarından yoksundurlar. Birçok KOBİ yöneticisi, şirketlerinde bilgi teknolojileri güvenliğinin temelde güvenlik duvarına sahip olmaya ve virüsten koruma yazılımını düzenli olarak güncellemeye eşdeğer olduğuna inanmaktadır. Stratejik politikalar, bilgi hırsızlığı, iş sürekliliği, erişim kontrolleri ve diğer pek çok husus sadece güvenlik ihlali durumunda ele alınmaktadır (Park ve Diğ., 2008).

KOBİ yöneticileri için bilgi güvenliği, yapılacak işler öncelik sıralamasında en gerilerde kalmaktadır. KOBİ yöneticileri, genel olarak bilgi güvenliğinin ve örgütlenmenin önemine inanmalarına rağmen gerekli tedbirleri almakta reaktif davranmaktadırlar (Abbas, Mahmood ve Hussain, 2015).

Bilgi ve iletişim teknolojisindeki gelişmeler her geçen gün yeni ürünler ve hizmetler sunmakla birlikte bu yenilikler beraberinde yeni riskler getirmektedir. Avrupa'da bulunan KOBİ'ler üzerine yapılan bir araştırmada; KOBİ'lerin bilgi teknolojileri güvenliği seviyesinin iyi bir noktaya işaret etmediği, bulut teknolojisi *(cloud computing)* ve kendi bilgisayarını getir *(BYOD, bring your own device)* uygulamasının yaygın bir şekilde kullanıldığı ancak, KOBİ'lerin bu yeni teknolojilerin getirdiği risklerin farkında olmadığı belirtilmiştir (Amrin, 2014) .

Bilgi ve iletişim teknolojisinin getirdiği yenilikler beraberinde belirsizlikleri de getirmektedir. Bu belirsizlikler kötü niyetli kişiler tarafından yönetildiği takdirde işletmelerin karşısına risk olarak çıkmakta, zamanında gerekli tedbirleri almayan işletmeler için kötü sonuçlara sebebiyet verebilmektedir.

Makalenin geri kalanı şu şekilde organize edilmiştir. Bölüm 2'de KOBİ'lerin bilgi güvenliğine ihtiyaç duyma sebeplerinden ve bilgi güvenliğinin benimsenmesinin önündeki zorluklardan bahsedilmiştir. Bölüm 3'te bilgi güvenliği risk çerçeveleri, Bölüm 4'te bilgi güvenliği program çerçeveleri ve Bölüm 5'te bilgi güvenliği kontrol çerçevelerine ilişkin örnekler ve bu örnekler hakkında bilgi verilmiştir. Bölüm 6'da KOBİ'lerin özelliklerinden yararlanılarak risk profillerinin belirlenmesine çalışılmıştır. Bölüm 7'de ise nitel değerlendirme yöntemine göre risk profillerinin derecelendirilmesine ve derecelendirilen risk profiline göre KOBİ'ler için uygun bilgi güvenliği çerçevesi seçimi hakkında önerilerde bulunulmuştur.

2. Kobiler ve Bilgi Güvenliği

2.1. KOBİ'lerin bilgi güvenliğini dikkate almasını gerektiren sebepler

Bilgi ve iletişim teknolojisindeki hızlı gelişimden nasıl büyük küçük demeden tüm işletmeler faydalanıyorlarsa, aynı şekilde bu gelişimden kaynaklanan siber tehdit ortamı yine büyük küçük demeden tüm işletmeleri tehdit etmektedir. Yeni teknolojilerin kullanımı, işletme faaliyetleri için fırsatlar sunduğu gibi azaltılması gereken potansiyel güvenlik riskleri de sunmaktadır. İstenmeyen olaylardan kasıtlı müdahalelere kadar bilgi güvenliğine yönelik tehditler günümüzde tüm kuruluşlar için ciddi riskler barındırmaktadır. Güvenlik önlemlerinin alınmaması her işletme için olduğu gibi KOBİ'ler için de geri dönülmesi imkânsız ticari ve itibari kayıplara yol açabilmektedir. Bilgi güvenliğine ilişkin standartların uygulanması bu risklerin daha oluşmadan tedbir alınması ve risk etkilerinin hafifletilmesi için çok önemlidir (Manso ve Diğ., 2015).

Birçok KOBİ temel ticari faaliyetler için elektronik tabanlı bilgi sistemlerine güvenmektedir. Etkin bir bilgi güvenliği, doğru, güvenilir ve kesintisiz işlemler sağladığı gibi ekipman veya veri hırsızlığından kaynaklanan zararları önler, bilgisayar virüsleri gibi olaylardan kaynaklanan zaman kaybını azaltır (ISSA, 2011).

Bazı durumlarda işletmelerin, bir faaliyette bulunmak istediklerinde bilgi güvenliği tedbirlerini aldıklarını ve uyguladıklarını ispatlamaları istenmektedir. Örneğin; bir firma e-Devlet Kapısı İhalesine girmek istediğinde, ihaleyi açan kuruluşun istediği özelliklere uymak bakımından ISO/IEC 17799 sertifikasını almak zorunda kalmıştır. Yine öte yandan e-İmza Yönetmeliği uyarınca bir işletmenin elektronik sertifika hizmet sağlayıcısı olabilmesi için ISO/IEC 27001 sertifikasının olması gerekmektedir (Ersoy, 2012).

Yapılan araştırmalar; çevrimiçi alışveriş yapan insanların; ödeme bilgilerinin ve kişisel verilerinin nasıl korunduğuna dair endişeler yaşadıklarını göstermektedir. Bilgi güvenliğini sağlayan işletmeler için bu özellikleri bir avantaj olmakta ve müşteriler tarafından bir tercih edilme nedeni olarak karşımıza çıkmaktadır. Bilgi güvenliğini sağlayacak tedbirlerin alınması ve bu olgunun paydaşlara sunulması KOBİ'lere katma değer sağlayacak ve tercih edilme sebebi olacaktır (Manso ve Diğ., 2015).

Birçok ulusal ve uluslararası mevzuat ve işletmelerin içinde bulunduğu sektöre özgü düzenlemeler işletmeleri bilgi güvenliğine ilişkin tedbirler almaya zorlamaktadır. Gerekli yasal zorunluluklara uyulmaması sonucu işletmeler yaptırımlarla karşı karşıya kalabilirler. Yaptırımlara maruz kalmamanın en etkin çözümlerinden biri de tüm dünyada kabul görmüş güvenlik standartlarını uygulamaktan geçmektedir. Yasal düzenlemeler her işletme gibi KOBİ'leri de kapsamaktadır (Manso ve Diğ., 2015).

Bilgi güvenliğine verilen önem ve önem verildiğinin müşterilere hissettirilmesi KOBİ'lere rekabet avantajı sağlayacak ve faaliyet gösterdiği sektörde güvenilir bir imaj yaratacaktır. Bilgi güvenliği standartlarına uyum hem tedarikçiler hem de müşteriler için bir güvence kaynağı olmaktadır (Manso ve Diğ., 2015; Ersoy, 2012).

Günümüzde, bankalar gibi sermaye sağlayıcılar, ihtiyaç sahibi KOBİ'nin risk profilini çıkarırken bilgi güvenliği durumuna da dikkat etmekte, bu konuda sertifikasyondan geçmiş olmak KOBİ'lerin daha kolay sermaye temin etmelerinde etken olmaktadır.

2.2. KOBİ'lerin bilgi güvenliğini benimsemesinin önündeki engeller

KOBİ'ler bilgi ve iletişimden kaynaklanan risklerin farkında olmakla birlikte bu riskleri bertaraf edecek, risk etkilerini hafifletecek bilgi güvenliği standartlarının farkında değildirler. KOBİ'lerin kullanabileceği standartlar sınırlı olmakla birlikte; çalıştıkları sektörün özelliklerini dikkate alan standartlar genelde yoktur ve KOBİ'lerin hedeflerini karşılayan standartların belirlenmesinde zorluklar yaşanmaktadır. Ayrıca KOBİ yöneticileri bu standartların işletmelerine sağlayacakları katma değerin farkında değildirler. Birçok araştırma bilgi güvenliği tehdidinin yalnızca büyük işletmeleri kapsadığı yönünde bir ön yargının olduğunu ve KOBİ'lerin bilgi güvenliğine yeterince eğilmediklerini göstermektedir (Manso ve Diğ., 2015). Bu araştırmalardan biri Amerika Birleşik Devletleri Ulusal Küçük İşletmeler Birliği (US National Small Bussiness Associaton, NSBA) tarafından 2013 yılında yapılan anket çalışmasıdır. Bu çalışmada, küçük işletmelerin sadece

%30'unun siber saldırılara karşı endişe duydukları, %60'ının ise bu konuda hafif endişeli oldukları, %11'inin ise hiç endişeli olmadıkları tespit edilmiştir. Bu yanlış kanı; KOBİ'leri bilgi güvenliği standartlarının temel olarak büyük şirketleri kapsadıkları ve kendilerine bir katma değer sağlamadıkları yönünde düşünmeye itmektedir (NSBA, 2013). KOBİ'lerde bilgi güvenliğine yatırım yapmak isteyen karar vericileri etkileyen faktörleri ortaya çıkarmak için çoklu vaka çalışması yaklaşımını benimseyen bir araştırmada katılımcılar "Küçük firma olmaları nedeniyle şanslı olduklarını, bilgisayar korsanlarının küçük işletmelerle ilgilenmediklerini ve saldırı olasılığının düşük olduğunu" ima etmişlerdir (Sean ve Diğerleri, 2013) . İngiltere merkezli BCRC (Business Crime Reduction Centre) tarafından bir araştırma projesini desteklemek amacıyla KOBİ odaklı gruplarla yapılan görüşmede "Asla başımıza gelmeyecek"; "Neden biri iş ve bilgisayar sistemlerimizi hedef almak istesin?"; "İşletmenin, bir bilgisayar korsanının çalmak isteyeceği hiçbir şey yok" ve "Tehdit nedir? Onu göremiyorum!" gibi bilgi güvenliğini önemsemediklerini gösteren yorumlarla karşılaşılmıştır (Lacey ve James. 2010).

Birçok KOBİ yöneticisi büyük şirketleri siber saldırıların hedeflerinde görmekte, kendilerinin ise bu saldırıların hedefinde olmadığını düşünmektedirler. Bu nedenle yapılacaklar listesinde bilgi güvenliği önceliği gerilerde kalmaktadır (Park ve Diğ., 2008).

KOBİ'ler bilgi güvenliğinin sağlanması bakımından özellikleri nedeniyle özel bir organizasyon kategorisinde bulunmaktadırlar. Kaynak kısıtlılığı, yetersiz bilgi birikimi nedeniyle etkili ve verimli bir bilgi güvenliği kontrol oluşturmada zorluklarla karşılaşmaktadırlar. Bu sorun bilgi güvenliğine ilişkin standartların ve yönergelerin çokluğunun yanında KOBİ'lerde yeterli uzman bulunmaması nedeniyle daha da derinleşmektedir. KOBİ'lerin çoğu, "bilgi güvenliği tehdidi sadece büyük şirketleri hedef alır" algısı nedeniyle temel bilgi güvenliği kontrollerinin bile uygulanmasını göz ardı ettiği için riskler daha da önemli hale gelmektedir (Gordas, 2014).

Mevcut iş çevresinde bir çok organizasyon ISO 27000X serisi, COBİT ve bunlar gibi çerçeveleri kendilerini bilgi güvenliği risklerine karşı korumak için kullanmaktadırlar. Ancak bu standartlar ve çerçeveler KOBİ'ler için çok karmaşıktırlar ve ihtiyaçlarına cevap vermemektedirler (Mijnhardt ve diğ., 2016).

Bilgi güvenliğine ilişkin birçok standart, karmaşık olmakla birlikte uzmanlık gerektirmektedir ve büyük işletmelerin özelliklerine göre tasarlanmıştır (Tawileh, Hilton ve McIntosh, 2007; Manso ve Diğ., 2015; Mijnhardt , Thijs ve Spruit, 2016). Tablo-1'de bilgi güvenliğine ilişkin Avrupa menşeli bazı standartlar sunulmuştur. Bu standartların çokluğu dikkat çekmekte olup, uygulanması mali külfet arz etmekte ve yeterli uzman personeli bulunmayan KOBİ'ler için bu standartların uygulanması zorluklar içermektedir.

Tablo 1. Bilgi güvenliğine ilişkin standartlar (Manso ve Diğ., 2015)

Bilgi Güvenliği
• IEC 27001: 2013 Bilgi güvenliği yönetim sistemleri – Gereksinimler
• ISO / IEC 27002: 2013 Bilgi güvenliği kontrolleri için uygulama kuralları
• ISO / IEC 27003: 2010 Bilgi güvenliği yönetim sistemi uygulama rehberi
• ISO / IEC 27004: 2009 Bilgi güvenliği yönetimi – Ölçme
• ISO / IEC 27013: 2012 Entegre uygulamasına dair rehber bilgiler ISO / IEC 27001 ve ISO / IEC 20000-1
• ISO / IEC 27014: 2013 Bilgi güvenliği yönetimi
• ISO / IEC TR 27016: 2014 Bilgi güvenliği yönetimi – Organizasyonel ekonomi
• ISO / IEC 27032: 2012 Bilgi güvenliği için yönergeler
• ISO / IEC 27033-1: 2009 Ağ güvenliği – Bölüm 1: Genel bakış ve kavramlar
• ISO / IEC 27033 -2: 2012 Ağ güvenliği – Bölüm 2: Ağ güvenliğinin tasarlanması ve uygulanması için yönergeler

• ISO / IEC 27033-3: 2010 Ağ güvenliği – Bölüm 3: Referans ağ oluşturma senaryoları – Tehditler, tasarım teknikleri ve kontrol sorunları • ISO / IEC 27033-4: 2014 Ağ güvenliği – Bölüm 4: Güvenlik ağ geçitleri kullanan ağlar arasında iletişimi sağlama • ISO / IEC 27033-5: 2013 Ağ güvenliği – Bölüm 5: Sanal Özel Ağlar (VPN) kullanarak ağlar arasında iletişimi sağlama • ISO / IEC 27034-1: 2011 Uygulama güvenliği – Bölüm 1: Genel bakış ve kavramlar • ISO / IEC 27039: 2015 İzinsiz giriş algılama sistemlerinin (IDPS) seçimi, dağıtımı ve işlemleri • ISO / IEC 27040: 2015 Depolama güvenliği • Cloud Security Alliance (CSA) Cloud Controls Matrisi • BSI PAS 555: 2013 Siber güvenlik riski. Yönetişim ve yönetim Teknik Özellikler • PCI Veri Güvenliği Standardı • ISF Bilgi Güvenliği için İyi Uygulama Standardı • UK Hükümet Güvenlik Politikası Çerçevesi • UK Gov. Cyber Essentials Şeması • ETSI GS ISI 001 Bölüm 1: Tam Kuruluşların güvenlik duruşlarını ölçmek için kullanacakları operasyonel göstergeler kümesi • ETSI TR 103 305 Etkin Siber Savunma için Kritik Güvenlik Kontrolleri • BSI 100-1 Bilgi Güvenliği Yönetim Sistemleri (ISMS) • BSI 100-2: IT –Grundschutz Metodolojisi
Risk Yönetimi
• ISO / TR 31004: 2013 Risk yönetimi – ISO 31000 uygulaması için rehberlik • ISO / IEC 27005: 2011 Bilgi güvenliği risk yönetimi • ISO / IEC 31000 Risk yönetimi – Risk değerlendirme teknikleri • IEC 31010: 2009 Risk yönetimi – Risk değerlendirme teknikleri • BSI BIP 0076 Bilgi güvenliği risk yönetimi. ISO / IEC 27001 için El Kitabı • BSI 100-3: IT-Grundschutz'a dayalı Risk Analizi
İş Sürekliliği Yönetimi
• ISO 22301: 2012 İş sürekliliği yönetim sistemleri – Gereksinimler • ISO 22313: 2012 İş sürekliliği yönetim sistemleri – Rehberlik • ISO / IEC 27031: 2011 İş sürekliliği için bilgi ve iletişim teknolojisine hazırlık ilkeleri • BSI 100-4: İş Sürekliliği Yönetimi
Veri Koruma ve Gizlilik
• ISO / IEC 27018: 2014 Kişisel olarak tanımlanabilir bilgi işlemcileri olarak hareket eden kamu bulutlarında kişisel olarak tanımlanabilir bilgilerin korunması için uygulama kuralları • ISO / IEC 29100: 2011 Gizlilik çerçevesi

• ISO / IEC 29101: 2013 Gizlilik mimarisi çerçevesi • BSI BS 10012: 2009 Veri koruma. Kişisel bilgi yönetim sistemi için şartname • CEN CWA 16113: 2010 Kişisel Verilerin Korunması İyi Uygulamalar
Olay Yönetimi
• ISO / PAS 22399: 2007 Toplumsal güvenlik – olaya hazırlık ve operasyonel süreklilik yönetimi için kılavuz • ISO / IEC 27035: 2011 Bilgi güvenliği olay yönetimi • ISO / IEC 27037: 2012 Sayısal kanıtların belirlenmesi, toplanması, edinimi ve korunması için yönergeler
Üçüncü Taraf Yönetimi
• ISO / IEC 27036-1: 2014 Tedarikçi ilişkileri için bilgi güvenliği – Bölüm 1: Genel bakış ve kavramlar • ISO / IEC 27036-2: 2014 Tedarikçi ilişkileri için bilgi güvenliği – Bölüm 2: Gereksinimler • ISO / IEC 27036-3: 2013 Tedarikçi ilişkileri için bilgi güvenliği – Bölüm 3: Bilgi ve iletişim teknolojisi tedarik zinciri güvenliği için kılavuzlar
Bazı Sektörlere Özgü Standartlar
• ISO / TR 13569: 2005 – Finansal hizmetler – Bilgi güvenliği yönergeleri [Finansal Hizmetler] • ISO / IEC TR 27015: 2012 – Finansal hizmetler için bilgi güvenliği yönetimi yönergeleri [Finansal Hizmetler] • ISO / IEC TR 27019: 2013 – Enerji hizmet sektörüne özgü proses kontrol sistemleri için ISO / IEC 27002'ye dayanan bilgi güvenliği yönetimi yönergeleri [Enerji] • ISO 27799: 2008 – ISO / IEC 27002'yi kullanarak sağlıkta bilgi güvenliği yönetimi [Sağlık Hizmetleri] • ISO 22307: 2008 Finansal hizmetler – Gizlilik etki değerlendirmesi [Finansal Hizmetler]

Bilgi güvenliğine ilişkin faaliyetlerin yürütülmesi zaman ve uzman işgücü kaynağı gerektirmektedir. Ayrıca bilgi güvenliği için gereken yatırım maliyetinden KOBİ'ler genellikle kaçınma eğilimi içerisindedirler (Tawileh, Hilton ve McIntosh, 2007; Manso ve Diğ., 2015).

Son yıllarda kişisel verilerin korunmasına yönelik birçok standart oluşturulmasına rağmen bu standartlar daha çok büyük şirketler için tasarlanmışlardır. Küçük organizasyonlara kişisel verilerin uygun şekilde işlenmesi, depolanması ve korunmasını sağlamaya yardımcı olmak için tasarlanan uluslararası standartlar oldukça sınırlıdır (Manso ve Diğ., 2015).

KOBİ'lerde bilgi güvenliğinin teknik yönü ağır basmakta, bütünsel bir yaklaşımla bakılmamakta, yönetsel yönü genellikle unutulmaktadır (Soomro , Shah ve Ahmed, 2016).

3. Bilgi Güvenliğine İlişkin Risk Çerçeveleri

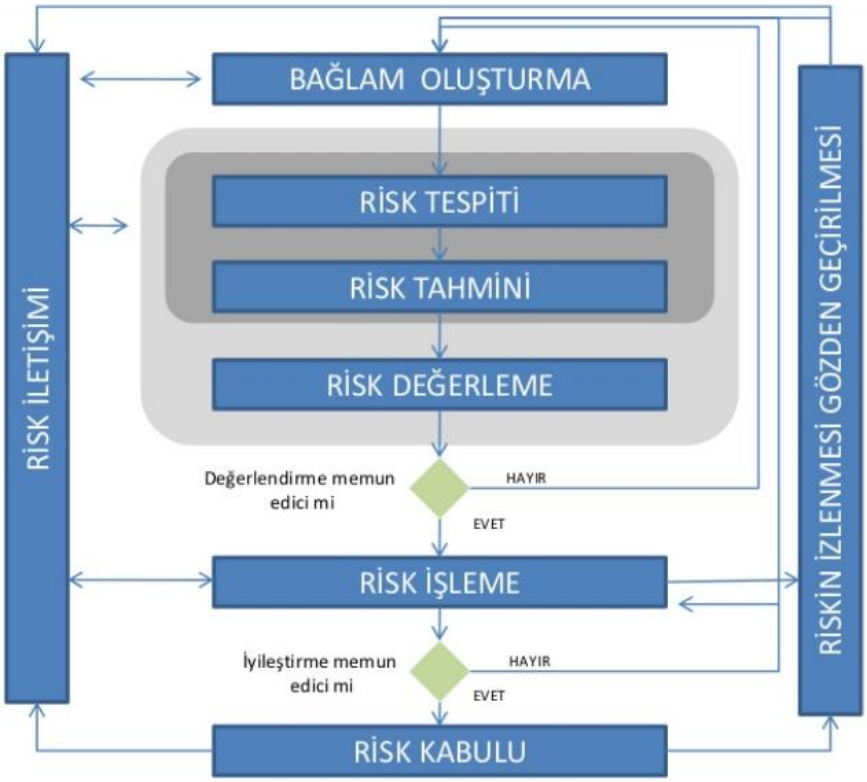
3.1. ISO 27005 bilgi güvenliği risk yönetimi (ISO 27005 Information Technology - Security Techniques - Information Security Risk Management)

ISO 27005 standardı, Uluslararası Standardizasyon Örgütü (ISO, International Organization for Standardization) tarafından yayınlanan, bilgi güvenliği konusunda kılavuz olarak tasarlanmış standartlar dizisidir. Risk yönetimi yaklaşımına uygun olarak bilgi güvenliği konusunda

organizasyonlara yardımcı olacak rehber niteliğindedir. ISO 27005 tarafından açıklanan metodolojide özetle; risk altındaki bilgi varlıkları, potansiyel tehditler veya tehdit kaynakları, potansiyel zayıf noktaları ve risklerin gerçekleşmesi durumunda ortaya çıkabilecek olası sonuçlar tanımlanmaya çalışılmaktadır. ISO 27005 detaylı, kalıplaşmış bilgiler yerine, esnek, yapılandırılabilir, organizasyonların kendileri tarafından, kendi ihtiyaçlarına göre şekillendirilebilecek bilgiler ihtiva eder. ISO 27005 standardı niceliksel ve niteliksel risk değerlendirme yöntemleri hakkında bilgi içermez, her ikisinin de riskleri tanımlamak yerine riskleri tahmin etmenin uygun yöntem olduğunu belirtir (Haythorn, 2015). ISO 27005 standartları, ISO / IEC 27001'in terminolojileri, bilgi kavramları, modelleri, süreçleri üzerine kuruludur.

ISO 27005, insanlar, süreçler ve teknoloji tüm örgütsel yönleri hesaba katan yapısal, sistematik ve titiz bir risk değerlendirme sürecinin ana hatlarını verirken, bunu gerçekleştirmek için teknik detaylara sahip yöntem sunmaz. Daha çok üst seviye yönetim uygulamalarına yöneliktir (Tewari, 2019).

Şekil 1. ISO 27005 Risk yönetim akışı



Kaynak: Al-Safwani, Hassan ve Katuk, 2014

3.2. NIST SP 800-30 bilgi teknoloji sistemleri için risk yönetim rehberi (NIST SP 800-30 Risk Management Guide for Information Technology Systems)

1901 yılında Amerika Birleşik Devletlerinde teknoloji ve standart gereksinimlerini karşılamak maksadıyla Ulusal Teknoloji ve Standartlar Enstitüsü [The National Institute of Standards and Technology (NIST)] kurulmuştur. Bu kuruluşun misyonu; yaşamın kolaylaştırılması için bilim, teknoloji ve standart geliştirmek olarak belirlenmiştir. Bu misyonun hayata geçirilmesi maksadıyla alt çalışma grupları oluşturulmuştur. Bu alt çalışma gruplarının bir tanesi de bilgisayar üzerine olan Bilgisayar Güvenlik Grubu'dur (Jansen ve Scarfone, 2008). NIST SP 800-30, 2002 yılında Amerika Birleşik Devletleri hükümeti tarafından çıkarılan Federal Bilgi Güvenliği Yasası [The Federal Information Security Management Act (FISMA)] uyarınca Ulusal Teknoloji ve Standartlar Enstitüsü [The National Institute of Standards and Technology (NIST)] Bilgisayar Güvenlik Grubu tarafından geliştirilmiştir. Daha çok kamu kuruluşları için tasarlandığından güvenlik kontrollerini detaylandırır ve kontrollerin yeterliliği üstünde çok durur (Haythorn,

2015). Özel sektörde de kullanılabilir. Bilgisayar güvenliğinde risk yönetimi ve risk değerlendirmesi kapsamında nelerin göz önünde bulundurulması gerektiğine dair çok ayrıntılı rehberlik ve tanımlama sağlar. Ayrıntılı kontrol listeleri, grafikler (akış şeması dâhil) ve matematiksel formüller içerir (Stoneburner, Goguen ve Feringa, 2002).

NIST SP 800-30 belgesi, BT altyapısını tamamen teknik bir bakış açısıyla korumak için tavsiye niteliğinde bir kılavuzdur. NIST SP 800-30 ilk risk değerlendirme standartlarından biridir ve diğer birçok standardı da etkilemiştir. NIST SP 800-30, üç farklı aşamada dokuz adımı içerir (Shanthamurthy, 2011) :

- Belirleme (Sistem karakterizasyonu, Tehdit tanımlama, Güvenlik açığı tespiti, Kontrol analizi)
- Analiz (Olabilirlik belirlenmesi, Risk belirleme)
- Azaltma (Kontrol önerileri, risk dokümantasyonu)

NIST SP 800-30 ayrıca, kuruluşlara sürekli olarak izlenmesi gereken belirli risk faktörlerini belirleme konusunda rehberlik sağlar, böylece kuruluşlar risklerin kabul edilemez seviyelere yükselip yükselmediğini (ör: kurumsal risk toleransını aşma) ve farklı işlemlerin gerçekleştirilmesi gerektiğini belirleyebilirler (NİST, 2012).

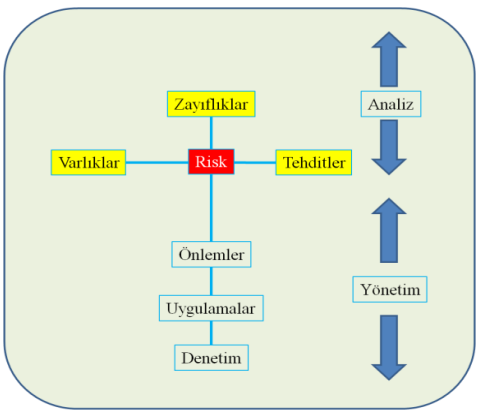
3.3. CRAMM risk analiz ve yönetim metodu [CRAMM- (CCTA) Central Computer and Telecommunication Agency Risk Analysis and Management Method]

İngiliz resmi telekomünikasyon kurumu tarafından 1987 yılında geliştirilmiştir. Nitel yönteme dayanın bir risk çerçevesidir. CRAMM (CCTA Risk Analysis and Management Method), devlet kurumları ve sanayi gibi büyük kuruluşlara yönelik olarak tasarlanmıştır (European Network and Information Security Agency).

Güvenlik tabanlı sorular kullanarak; organizasyona ilişkin varlıkları, işlemleri, uygulamaları, sistemleri, tehdit ve zayıflıkları, risk seviyeleri ile karşı tedbirleri analiz eder. Verilen cevaplar doğrultusunda, karşı tedbirleri değerlendirilir ve öncelikler belirlenir, koruyucu maliyetleri belirlenmeye çalışılır, güvenlik politikası belirlenmesine ve denetleme yapılması için yardımcı olur (Central Computer and Telecommunication Agency, 2009).

CRAMM, varlıkların tanımlanmasına ve değerlendirilmesine yardımcı olmak için önceden tanımlanmış 10 varlık tablosunu kullanarak nitel ve varlık merkezli bir yaklaşım benimsemiştir. ISO 27001 sertifikasıyla uyumlu olan CRAMM; varlık merkezli yaklaşımı ve varlık değerleme tekniği diğer metodolojilere de entegre edilmiştir (Houmb, 2007). Değerlendirmenin karmaşıklığının ihtiyaçlara göre ayarlanabilir olması, sürecin çoğunlukla yazılımla otomatik olarak yürütülmesi avantajları olarak sayılabilirken, uzman bilgisinin gerekmesi, değerlendirme çıktılarının karmaşık olması dezavantajları olarak karşımıza çıkabilir.

Şekil 2. CRAMM genel bakış



Kaynak: Mayer, 2009

CRAMM süreci üç ana aşamadan oluşmaktadır (Ionita ve Diğ., 2013):

- Varlık tespiti ve değerlemesi - Değerlendirmenin genel hedeflerini ve ayrıca sınırlarını belirledikten sonra, fiziksel ve yazılım varlıkları tanımlanır ve değerlenir.
- Tehdit ve güvenlik açığı değerlendirmesi - Bu adım, sisteme yönelik olası tehditleri tanımlayarak ve analiz ederek, sistemin bu tehditlere karşı kırılganlığını değerlendirerek ve son olarak riski hesaplamak için varlıklar, tehditler ve güvenlik açıkları hakkındaki bilgileri kullanarak, risklerin fiili değerlendirmesini kapsar.
- Karşı önlem seçimi ve öneri - Bu üçüncü aşama, mevcut azaltma stratejilerinin maliyet ve etkililiğini belirlemek ve sıralamak için CRAMM'in karşı önlem havuzunu kullanır.

3.4. FAIR bilgi riski faktör analizi (FAİR-Factor Analysis of Information Risk)

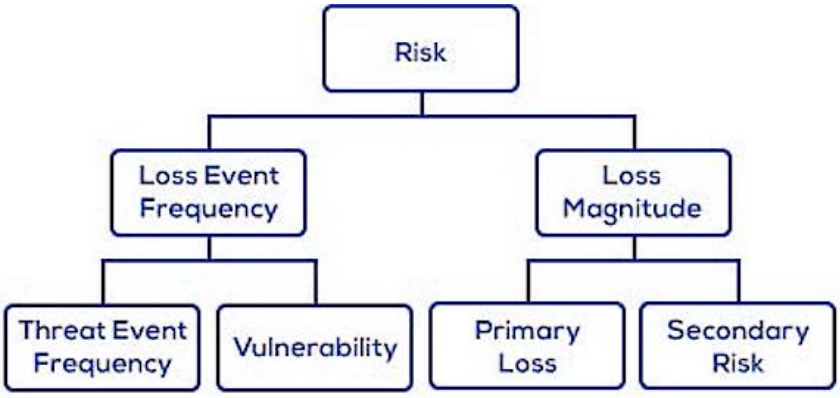
FAIR, riske katkıda bulunan faktörlerin sınıflandırılması ve bu faktörlerin birbirini nasıl tanımladığı üzerine kurulu bir risk çerçevesidir. FAIR öncelikle olumsuz olayların büyüklüğü ve sıklığı üzerine odaklanır (The Open Group, 2009). FAIR çerçevesi; tehditler, varlıklar, organizasyonun kendisi ve dış çevre olmak üzere bir risk senaryosunun dört ana bileşenini tanımlamaya çalışır (Risk Management Insight LLC., 2006).

FAIR Temel Risk Değerlendirme Rehberi, dört aşamaya yayılan bir süreci açıklar (Risk Management Insight LLC., 2006):

- Senaryo bileşenlerini tanımlayın
- Kayıp olay sıklığını değerlendirin
- Olası zarar büyüklüğünü değerlendirin
- Riski tanımlayın ve açıklayın.

FAIR metodolojisi diğer metodolojilerle doğrudan rekabet içinde değildir tam aksine NIST 800-30, ISO / IEC 27002, COBIT, ITIL veya COSO gibi risk yönetimi metodolojilerini tamamlar ve birlikte kullanılabilir. Temel risk değerlendirme işleminin hızlı olması ve özel araçlar veya özel eğitim gerektirmemesi avantaj olarak karşımıza çıkmaktadır (The Open Group, 2009).

Şekil-3 FAIR Risk Modeli Bileşenleri



Kaynak : FAIR Institute

3.5. OCTAVE operasyonel olarak kritik tehdit, varlık ve savunmasızlık değerlendirmesi (OCTAVE-Operationally Critical Threat, Asset and Vulnerability Evaluation)

OCTAVE, bilgi güvenliği risklerini tanımlamak ve değerlendirmek için bir geliştirilen bir metodolojidir. OCTAVE ile, kurumun operasyonel risk toleranslarını tanımlayan nitel risk değerlendirme kriterleri geliştirmek, kurumun misyonu için önemli olan varlıkları belirlemek, bu varlıklara karşı açıkları ve tehditleri belirlemek, tehditlerin gerçekleştirilmesi durumunda kuruluşun potansiyel sonuçlarını belirlemek ve değerlendirmek amaçlanmıştır (Caralli ve diğ., 2007).

OCTAVE, risk değerlendirmeleri için gerekli araç, teknik ve yöntemleri içerir. Carnegie Mellon Yazılım Mühendisliği Enstitüsü tarafından geliştirilmiştir ve birçok bilgi güvenliği uzmanı

tarafından kabul görmektedir (Haythorn, 2015). Çeşitli araç, teknik ve yöntemler içeren OCTAVE çerçevesi "risk tabanlı bilgi güvenliği stratejik değerlendirmesi ve planlaması"na uygun bir yapıdadır. OCTAVE çerçevesinin çeşitli versiyonları da bulunmaktadır: OCTAVE-S; daha çok küçük yapıdaki işletmelere göre tasarlanmışken, OCTAVE Allergo ise bilgi varlıkları üzerine yoğunlaşan hızlı bir çerçevedir (Ionita ve Diğ., 2013).

OCTAVE metodu üç aşamada gerçekleştirilir. 1. aşamada, analiz ekibi bilgi ile ilgili önemli varlıkları ve bu varlıklar için mevcut koruma stratejisini tanımlar. Ardından ekip, tanımlanmış varlıklardan hangisinin kuruluşun başarısı için en kritik olduğunu belirler, güvenlik gereksinimlerini belgeler ve bu gereksinimlerin karşılanmasına müdahale edebilecek tehditleri belirler. 2. aşamada, analiz ekibi 1. aşamada gerçekleştirilen tehdit analizini desteklemek ve 3. aşamada azaltma kararlarını bildirmek için bilgi altyapısının değerlendirmesini yapar. Son olarak, 3. aşamada, analiz ekibi risk tanımlama faaliyetlerini gerçekleştirir ve bir risk azaltma geliştirir. Kritik varlıklar için risk azaltmaya yönelik planlama yapar (Alberts ve Dorofee, 2002).

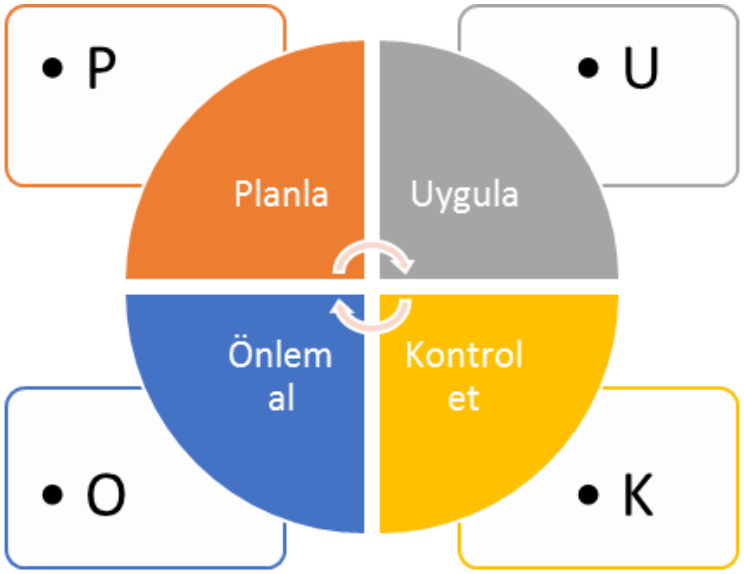
4. Bilgi Güvenliğine İlişkin Program Çerçeveleri

4.1. ISO/IEC 27001 bilgi teknolojisi-güvenlik teknikleri-bilgi güvenliği yönetim sistemleri-gereksinimler (ISO/IEC 27001 Information technology -- Security techniques -- Information security management systems -- Requirements)

ISO 27000 ailesinden gelen ve ISO/IEC 17779'un yerini alan bu program çerçevesi, bilgi güvenliği yönetimimin nasıl daha iyi hale getirileceği üzerine kuruludur. Teknik bir standart değildir. Genel bir çerçeve çizer ve işin nasıl yapılacağını ilgili işletmeye bırakır.

Sürekli iyileştirme metodu olarak: planla, uygula, kontrol et, önlem al döngüsünü esas almıştır. Bu döngü durmaksızın devam eder. Hedef her seferinde daha iyi bir güvenlik sisteminin kurulması ve idamesidir (Marttin ve Pehlivan, 2010) .

Şekil 4. PUKÖ Döngüsü



Kaynak: ASQ

ISO 27001 ile, yaşayan, gelen tehdit ve saldırılara karşı tepki veren ve bu tepkilere göre kendisini yenileyen bir bilgi güvenliği sisteminde olması gereken öğeleri tanımlanmaya çalışılır. ISO 27001'de tanımlanmaya çalışan yaklaşım için bilgi güvenliğinin bir süreç olarak ele alınması gerekmektedir. Sürecin planlama, uygulama, kontrol etme ve önlem alma basamaklarından oluşan bir çark şeklinde çalıştırılması ve her yeni durum için kendini yenileyecek şekilde çalışması önem arz etmektedir. Bu döngünün devam ettirilmesi sürecin hayatta kalabilmesi için gereklidir (Ottekin, 2008).

ISO 27001 genellikle ISO 27002 standardı ile birlikte yürütülür. ISO 27001 bilgi güvenliği gereksinimlerini tanımlamaya çalışırken, bilgi güvenliği denetimleri için de ISO 27002'deki ana hatları kullanır (Öztürk, 2008).

4.2. NIST siber güvenlik çerçevesi (NIST, National Institute of Standards and Technology Cybersecurıty Framework)

ABD Ulusal Standartlar ve Teknoloji Enstitüsü (NIST, National Institute of Standards and Technology) tarafından 2014 yılında yayımlanmıştır. Bu çerçeve; siber güvenlik riskini daha iyi yönetmek ve azaltmak için mevcut standartlara, kılavuzlara ve uygulamalara dayalı gönüllü rehberlik etmek, hem iç hem de dış kurumsal paydaşlar arasında risk ve siber güvenlik yönetimi iletişimini teşvik etmek için tasarlanmıştır (NIST, 2016).

NIST üç bölümden oluşur. Birinci bölüm; arzu edilen, hedeflenen güvenliğin ne olduğunun tanımlandığı çekirdek bölümüdür. Belgenin merkezi kısmı olan CSF Çekirdeği, belirli bir siber güvenlik sonuçlarını elde etmek için bir dizi etkinlik sağlayan 5 temel işlevi, 23 kategoriyi ve 108 alt kategoriyi açıklar (Zaras, 2018).

Şekil 5. NİST Çekirdeğindeki 5 temel işlev

Kaynak: Hanacek, 2018

İkinci bölüm; bireysel bir organizasyonun kendine özgü gereksinimlerinin, hedeflerinin, risk iştahının ve kaynaklarının tanımlandığı profil bölümüdür. Üçüncü bölüm ise; işletmenin siber güvenlik risklerini nasıl yönettiğini gösteren uygulama katmanları bölümüdür (Zaras, 2018).

Süreç açısından bakıldığında NIST siber güvenlik çerçevesi; organizasyonun misyonunu ve risk toleransını anlamaktan başlar. Bunun bir kısmı, kuruluşun kritik altyapıdaki rolünü anlamaktır. Bunlar roller, sorumluluklar, politikalar ve süreçleri tanımlamak için kullanılır. Siber güvenlik, teknik kontroller, izleme ve planlı cevaplar olarak gerçekleştirilir. Süreçler tecrübeye göre gözden geçirilir ve geliştirilir. Teknik açıdan bakıldığında ise siber güvenlik, kimlikleri, kimlik bilgilerini ve ayrıcalıklarını ve ilgili erişimlerini yönetmekten başlar (Secure Shell, 2018).

4.3. HITRUST Siber Güvenlik Çerçevesi (HITRUST Cybersecurity Framework)

Amerika Birleşik Devletleri merkezli, bağımsız ve kar amacı gütmeyen HITRUST Alliance isimli organizasyon tarafından hem özel sektör ham de kamu için geliştirilmiş risk ve uygunluk yönetim çerçevesidir.

Karmaşık olan gereksinimleri, basit ve tek bir çerçevede toplamayı, birleştirmeyi amaçlamışlardır. İlk başlarda sağlık sektörüne odaklanmışlarken zamanla yaşanan gelişmelerle finansal sektör de çerçeve kapsamına girmiştir (Zaras, 2018).

HITRUST CSF çerçevesi, ISO / IEC 27001: 2005 ve 27002: 2005'e dayanan 46 Kontrol Amacı ve 149 Kontrol tanımından oluşan 14 Kontrol Kategorisi içerir. Bu kontrol kategorileri: Bilgi Güvenliği Yönetimi Programı, Erişim Kontrolü, İnsan Kaynakları Güvenliği, Risk Yönetimi, Güvenlik Politikası, Bilgi Güvenliği Organizasyonu, Uyumluluk, Varlık Yönetimi, Fiziksel ve Çevre Güvenliği, İletişim ve İşlem Yönetimi, Bilgi Sistemleri Satın Alma, Geliştirme ve Bakım, Bilgi Güvenliği Olay Yönetimi, İş Sürekliliği Yönetimi ile Gizlilik Uygulamaları'dır (Kirkpatrickprice, 2019).

Çerçevenin dokuzuncu versiyonu ayrıca, siber güvenlik riskleri ile ilgili rehberlik sağlayan Ulusal Standartlar Enstitüsü ve Teknolojinin (NIST) Siber Güvenlik Çerçevesinin hedeflerini de içermektedir (Cohen, 2017).

5. Bilgi Güvenliğine İlişkin Kontrol Çerçeveleri

5.1. İnternet güvenlik merkezi (CIS) kontrolleri (Center for Internet Security Controls, CIS CSC))

Bu kontroller, İnternet Güvenliği Merkezi (Center for Internet Security, CIS) tarafından tasarlanmışlardır. İnternet Güvenliği Merkezi, özel ve kamu kuruluşlarını siber tehditlere karşı korumak için tedbirler geliştiren, kar amacı gütmeyen bir kuruluştur. Yayınlanan 20 kontrol ve bunlara bağlı alt kontroller uygulandığı takdirde nerdeyse tüm bilgi güvenliği risklerinin karşılanacağı varsayılmaktadır. Yine bu kontrollerden ilk beşi uygulandığı takdirde birçok bilgi güvenliği riskinin azaltılacağı belirtilmektedir (Zaras, 2018).

20 Kontrol grubu, kişisel bilgileri toplayan veya muhafaza eden herhangi bir kuruluşun yerine getirmesi gereken minimum güvenlik seviyesini teşkil eder (Harris, 2016).

Önceliklendirme, CIS kontrollerine uygulanmasında önemli bir faktördür. Kuruluşlara savunmalarının başlangıç noktasını hızlı bir şekilde tanımlamalarına yardımcı olmak, kıt kaynaklarını derhal ve katma değeri yüksek aksiyonlara yönlendirmek, dikkatlerini ve kaynaklarını işlerine veya görevlerine özgü ek risk konularına odaklamak üzere tasarlanmıştır.

Toplamda 20 CIS kontrolü var; ilk altı kontrol, siber savunma hazırlığı için tüm kuruluşlar tarafından uygulanması gereken "temel" kontroller olarak belirlenmiştir. Bu ilk altı CIS kontrolü şunlardır: Donanım Varlıklarının Envanteri ve Kontrolü, Yazılım Varlıklarının Envanteri ve Kontrolü, Sürekli Güvenlik Açığı Yönetimi, İdari Ayrıcalıkların Kontrollü Kullanımı, Mobil Cihazlarda, Dizüstü Bilgisayarlarda, İş İstasyonlarında ve Sunuculardа Donanım ve Yazılım İçin Güvenli Yapılandırma, Denetim Günlüklerinin Bakım, İzleme ve Analizi. Her kontrol kapsamlıdır. Güvenliğe veri, yazılım ve donanım odaklı olarak bakmaz aynı zamanda insanları ve süreçleri de katar. Örneğin, her iki güçlü proaktif savunma planının ana bileşenleri olan Olay Müdahale ekipleri ve Kırmızı ekipler sırasıyla 19 ve 20 numaralı CIS kontrollerinde bulunmaktadır (Rapid7).

5.2. NIST SP 800-53 (NIST Special Publication (SP) 800-53)

NIST SP 800-53, Amerika Birleşik Devletleri federal bilgi sistemleri için güvenlik kontrolleri kataloğu sağlayan belgedir. Her ne kadar bu kontroller kamu kuruluşları için tasarlanmışsa da özel sektörün de kullanmasını engelleyen bir tahdit yoktur ve bir çok özel kuruluş tarafından da kullanılmaktadır. Bu kontrol grubu; ulusal ve uluslararası gereksinimleri karşılayan 20 kontrol ailesinden oluşmaktadır. Bu kapsamlı kontrol kataloğunu derlemek için savunma, finansal, sağlık, üretim, sanayi ve denetim topluluklarından gelen gereksinimler ve kontroller kullanılmıştır (Zaras, 2018).

NIST SP 800-53, bilgi sistemleri tarafından federal bilgi sistemlerinin bütünlüğünü, gizliliğini ve güvenliğini sağlamak için kullanılan operasyonel, teknik ve yönetim önlemleridir. NIST kuralları, kontrol uyumluluğuyla risk yönetimine çok katmanlı bir yaklaşım benimsemiştir. SP 800-53, federal kurumlara ve yüklenicilere risk yönetimi programlarının uygulanması konusunda

rehberlik etmek üzere geliştirilen SP 800-37 ile birlikte çalışır. SP 800-53, 800-37'de belirtilen risk yönetimi çerçevesi ile birlikte kullanılabilecek kontrollere odaklanır (Lord, 2018).

5.3. ISO/IEC 27002 bilgi teknolojisi - güvenlik teknikleri - bilgi güvenliği kontrolleri için uygulama kodu (ISO/IEC 27002 Information technology - Security techniques - Code of practice for information security controls)

Bu Uluslararası Standart, organizasyonun bilgi güvenliği risk ortamını / ortamlarını göz önünde bulunduran kontrollerin seçimi, uygulanması ve yönetimi dâhil olmak üzere, organizasyonel bilgi güvenliği standartları ve bilgi güvenliği yönetimi uygulamaları için kılavuzlar sunar.

ISO/IEC 27002'nin ne olduğunu anlayabilmek için ISO/IEC 27001 ve ISO/IEC 27002 arasındaki ilişkiyi anlamak önemlidir. ISO/IEC 27001, bilgi güvenliği yönetim sisteminin tasarımına odaklanan bir standart dizisi iken; ISO/IEC 27002, bu bilgi güvenliği yönetim sisteminin en iyi nasıl kurulabileceğine ilişkin kontrolleri barındırır. ISO 27001 sertifikasyonu almak isteyen bir işletmenin, ISO 27002'de belirtilen kontrolleri uygulaması kolaylık sağlar (Zaras, 2018).

ISO/IEC 27002 standardı 14 ana güvenlik kontrol maddesi ve bunlara ilişkin 35 ana güvenlik kategorisi ile 114 kontrol içerir. Kuruluşun amacına, özelliğine göre bir kontrol diğer kontrollere göre daha çok önem arz edebilir. Kontrollerin seçimi; kuruluşun risk yönetimine nasıl yaklaştığına bağlıdır. (TS ISO/IEC 27002, 2013)

6. Risk Profilinin Belirlenmesi

Bilgi riski profili, bir işletmenin bilgi riski yönetimi stratejisi ve faaliyetlerinin başarısı için kritik öneme sahiptir. Bir işletmenin bilgi riski iştahı ve bilgi riski yönetimi beklentileri hakkında değerli bilgiler sağlar, karar vericiler için risk yönetimine ilişkin önemli ipuçları verir (Pironti, 2013). KOBİ'lerin tanımlamaları yapılırken nitel ve nicel özelliklerinden yararlanılır. KOBİ'lerin risk profilinin belirlenmesinde bu nitel ve nicel özellikler ile KOBİ'nin faaliyet gösterdiği sektörün dikkate alınması risk değerlendirmesi yapılırken kolaylık sağlayacaktır.

F. Mijnhardt ve arkadaşları (2016) yaptıkları araştırmada KOBİ özelliklerinden yola çıkarak, KOBİ'lerin bilgi güvenliği olgunluklarının tespit edilmesinde kullanılabilecek organizasyon özelliklerinin tespit edilmesi üzerinde çalışmışlardır. Uzmanlarla yaptıkları görüşmede 26 özelliği incelemişlerdir. Bu özelliklerden uzman görüşlerine göre anlamlı olanlar ve risk profilinin tespit edilmesinde kullanılabileceği değerlendirilen özellikler aşağıdaki Tablo-2'de sunulmuştur.

6698 sayılı Kişisel Verilerin Korunması Kanunu gibi geneli ilgilendiren yasal mevzuat ile işletmenin faaliyet gösterdiği sektöre özgü mevzuat (sağlık sektörü gibi) KOBİ'ler için, eğer uygun tedbirler alınmazsa, risk oluşturmaktadır. Özellikle kişisel bilgilerin muhafazasının ihlali sonucu işletmeler yasal yaptırımlara maruz kalabilmektedirler. İşletmenin geliri/kazancı özellikle çalışan sayısı ile birlikte yorumlandığında işletmenin yapısı hakkında değerli bilgiler vermektedir. İşletme geliri artıyorsa bu işletmenin büyüklüğüne ve karmaşık bir yapıya sahip olduğuna dolayısıyla riskin artığına dair göstergelerinden biri olarak karşımıza çıkmaktadır. Bilgi teknolojileri kaynaklarına erişen çalışan sayısı arttıkça veri bütünlüğü, gizliliği ve erişebilirliğine ilişkin riskler de çoğalmaktadır. Bilgi teknolojileri olmadan işletmenin faaliyetlerine devam edebilme kapasitesi bilgi teknolojilerine olan bağımlılık derecesinin en iyi göstergelerinden biri olarak karşımıza çıkmaktadır. Bilgi teknolojilerine bağımlılık derecesi arttıkça, bilgi teknolojileri riskinden işletme faaliyetlerinin etkilenme olasılığı da artmaktadır.

Tablo 2. Risk profilinin tespit edilmesinde kullanılabilecek özellikler

Risk profilinin tespit edilmesinde kullanılabilecek özellikler	Konu Hakkında Yapılan Çalışmalar
• Yasal mevzuatın getirdiği yükümlülükler • Bilginin gizliliği, bütünlüğü, erişebilirliği	• (Kotulic ve Clarck, 2004) • (Kraemer, Carayon ve Clem, 2009) • (Rehage, Hunt ve Nikitin, 2008) • (Smith ve Jamieson, 2006) • (Guttman ve Roback, 1995) • (Whitman ve Mattford, 2011)
• İşletme Geliri/Kazancı	• (Ein-Dor ve Segev, 1978)
• Çalışan Sayısı	• (Kotulic ve Clarck, 2004) • (Smith ve Jamieson, 2006) • (Chang ve Ho, 2006) • (Dunkerley ve Tejay, 2011) • (Hanseth ve Ciborra, 2007) • (Kankanhalli, Teo, Tan, ve Wei, 2003)
• Bilgi sistemlerine bağımlılık derecesi	• (Rehage, Hunt ve Nikitin, 2008) • (Whitman ve Mattford, 2011) • (Hanseth ve Ciborra, 2007)
• KOBİ'nin faaliyet gösterdiği sektör (Sektöre özgü düzenlemeler /yaptırımlar)	• (Ein-Dor ve Segev, 1978) • (Chang ve Ho, 2006) • (Kankanhalli, Teo, Tan ve Wei, 2003)

Yukarıda verilen özellikler dikkate alındığında KOBİ yöneticisi bilgi güvenliği risk profilinin tespit edilmesinden önce şu sorulara cevap aramalıdır;

• İşletmemde yasal mevzuat ve tabi olduğum sektör gereği tutmam gereken kişisel bilgi/bilgi var mı?

• Çalışanların verilere ulaşma sıklığı ne kadar?

• Bilgi sistemleri olmadan işimi ne kadar sürdürebilirim? Müşteri kaybı ne zaman gerçekleşir? Operasyonlarım ne zaman durur?

• Bilgi sistemlerinin işletme kazancıma katkısı var mı?

Bu sorulardan yola çıkarak bir KOBİ yöneticisi için risk profilinin belirlenmesinde kolaylık sağlayacak şekilde tasarlanan özellikler gruplandırılarak Tablo-3'te sunulmuştur.

Tablo 3. Risk profilinin tespit edilmesinde kullanılabilecek özelliklerin gruplandırılması

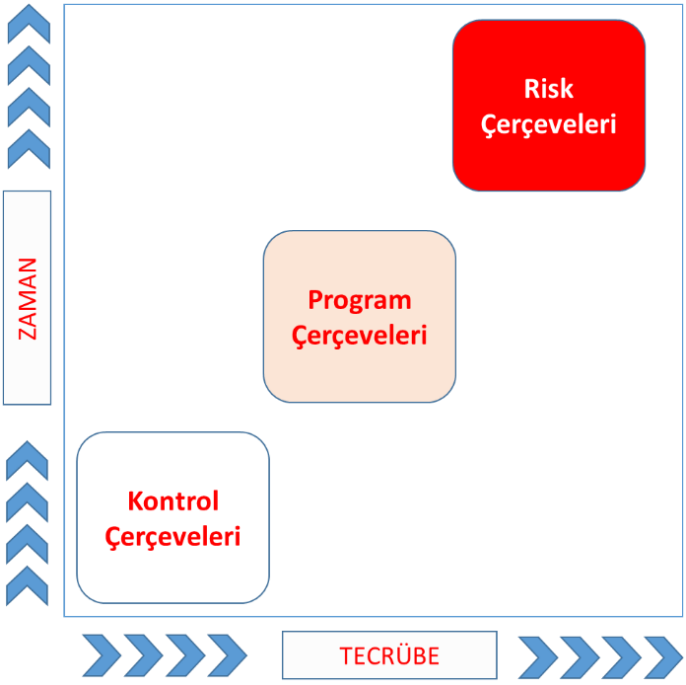
Mevzuat
• KOBİ'm 6698 sayılı Kişisel Verilerin Korunması Kanununda tanımlanan "**Veri Sorumlusu**"dur /Mevzuat gereği tutmam gereken özel bilgiler vardır. • KOBİ'm; 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında bulunmayan kişisel verileri tutmaktadır/tutmam gereken özel bilgiler vardır. • KOBİ'm; kendi çalışanlarına ait veriler dışında kişisel veri bulundurmamaktadır/tutmam gereken özel bilgi yoktur.
Çalışanların Verilere Erişim Sıklığı
• KOBİ'mde çalışanlardan en az 50 kişi günlük olarak veri tabanına erişebilmektedir. • KOBİ'mde çalışanlardan 50 kişiden daha az kişi günlük olarak olarak veri tabanına erişebilmektedir. • KOBİ'mde çalışanlardan 10 kişiden daha az kişi günlük olarak olarak veri tabanına erişebilmektedir.
KOBİ Geliri
• KOBİ'min Yıllık Net Satış Hâsılatı veya Yıllık Mali Bilanço Toplamı>25 Milyon TL • KOBİ'min Yıllık Net Satış Hâsılatı veya Yıllık Mali Bilanço Toplamı ≤ 25 Milyon TL • KOBİ'min Yıllık Net Satış Hâsılatı veya Yıllık Mali Bilanço Toplamı ≤ 3 Milyon TL
Sektöre özgü düzenlemeler
• KOBİ'm kişisel bilgileri tutan bir sektördedir. (Sağlık, ilaç, banka vb.) • KOBİ'm; kişisel bilgileri tutan bir sektörde değildir ancak yine de kişisel verileri tutmaktadır/tutmam gereken özel bilgiler vardır. • KOBİ'm; kişisel bilgileri tutması gereken bir sektörde değildir.
BT Kesintilerine Tahammül Derecesi
• BT kesintisi olduğu anda müşterilerimi kaybederim/operasyonlarım durur. • BT kesintisi 24 saatten fazla sürdüğü takdirde müşterilerimi kaybederim/operasyonlarım durur. • BT kesintisi olduğunda müşterilerimi kaybetmem/operasyonlarım devam eder.

7. Risk Profili Ve Çerçeve Seçimi İlişkisi

Bilgi güvenliğine ilişkin alınacak önlemler bağlamında bir çok yaklaşım bulunmaktadır. Bu yaklaşımlara bölüm 3, 4, 5'te değinilmiş ve üç kategori altında toplanmıştır. Bu yaklaşımlardan ilk kategori, kontrol çerçeveleridir. Kontrol çerçeveleri, her güvenlik programının temelini oluşturan güvenlik kontrollerini tanımlar. İkinci kategori olan program çerçeveleri, güvenlik programını yapılandırmaya, program faaliyetlerini değerlendirmek için bir temel oluşturmaya ve program hakkındaki iletişimi sadeleştirmeye yardımcı olur. Risk çerçeveleri ise, riski işletmeye değer sağlayacak şekilde yönetmek ve değerlendirmek için tutarlı bir yaklaşım sunar. Kontrol çerçeveleri az zaman ve az tecrübe gerektirirken, risk çerçevelerinin uygulanması daha karmaşıktır ve çok zaman ve uzmanlık gerektirir. Daha fazla zaman ve uzmanlık aynı zamanda

maliyet demektir. Şekil-5'te bilgi güvenliğine ilişkin çerçeveler arasındaki zaman-uzmanlık bağlamında ilişki gösterilmektedir (SANS, 2018).

Şekil 6 Bilgi güvenliği çerçeve kategorileri



Kaynak: SANS, 2018

Kontrol çerçevelerinin uygulanabilmesi için özel bir uzmanlık gerektirmemektedir. Basit bilgisayar okuryazarlığı olan ve gerektiğinde internet üzerinden araştırma yapabilen bir kişi tarafından kolaylıkla uygulanabilir. Ancak risk çerçevelerinin uygulanması ve hayata geçirilebilmesi için uzmanlık ve alan eğitimi gerektirmektedir. Risk çerçevelerinin kurum kültürüne adapte edilmesi, personel tarafından benimsenmesi zaman alır.

Bilgi güvenliği risk değerlendirilmesinde kullanılan nitel değerlendirme yönteminde risk seviyelerini üçe ayırmak mümkündür (Pironti, 2013). Bunlar;

- Yüksek — Şiddetli müşteri güven kaybı, marka itibar kaybı, varlıklar, kritik iş süreçleri ve/veya iş operasyonları üzerinde önemli maddi etki,
- Orta —Müşteri güven kaybı, marka itibar kaybı, varlıklar, kritik iş süreçleri ve/veya iş operasyonları üzerinde maddi etki,
- Düşük — Müşteri güveninde ve / veya marka itibarında önemsiz bir değişiklik, varlıklar, kritik iş süreçleri ve/veya iş operasyonları üzerinde asgari maddi etki.

6. bölümde risk profiline göre gruplandırılan özelliklerden "mevzuat" ve "sektöre özgü düzenlemeler" yakın ilişkili olduklarından dolayı birleştirilmiştir. Bu birleştirmeden sonra profiller nitel değerlendirme metodunda kullanılan "yüksek", "orta" ve "düşük" olmak üzere risk seviyelerine ayrılmıştır.

Tablo 4. Mevzuata ilişkin risk profili

1	KOBİ'm 6698 sayılı Kişisel Verilerin Korunması Kanununda tanımlanan "**Veri Sorumlusu**"dur/Mevzuat gereği tutmam gereken özel bilgiler vardır.	Yüksek
2	KOBİ'm; 6698 sayılı Kişisel Verilerin Korunması Kanunu kapsamında bulunmayan kişisel verileri tutmaktadır/tutmam gereken özel bilgiler vardır.	Orta
3	KOBİ; kendi çalışanlarına ait veriler dışında kişisel veri bulundurmamaktadır/tutmam gereken özel bilgi yoktur.	Düşük

Tablo 5. Gelire ilişkin risk profili

1	Yıllık Net Satış Hâsılatı veya Yıllık Mali Bilanço Toplamı>25 Milyon TL	Yüksek
2	Yıllık Net Satış Hâsılatı veya Yıllık Mali Bilanço Toplamı ≤ 25 Milyon TL	Orta
3	Yıllık Net Satış Hâsılatı veya Yıllık Mali Bilanço Toplamı ≤ 3 Milyon TL.	Düşük

Tablo 6. BT kaynaklarına erişime ilişkin risk profili

1	Çalışanlardan en az 50 kişi günlük olarak BT kaynaklarını kullanmaktadır.	Yüksek
2	Çalışanlardan 50 kişiden daha az kişi günlük olarak BT kaynaklarını kullanmaktadır.	Orta
3	Çalışanlardan 10 kişiden daha az kişi günlük olarak BT kaynaklarını kullanmaktadır.	Düşük

Tablo 7. BT kesintilerine tahammül derecesine ilişkin risk profili

1	BT kesintisi olduğu anda müşterilerimi kaybederim/operasyonlarım durur.	Yüksek
2	BT kesintisi 24 saatten fazla sürdüğü takdirde müşterilerimi kaybederim/operasyonlarım durur.	Orta
3	BT kesintisi olduğunda müşterilerimi kaybetmem/operasyonlarım devam eder.	Düşük

Bir KOBİ'de yukarıda belirtilen risk profili belirlendikten sonra risk seviyesi tespit edilerek uygulanabilecek çerçeve seçilebilir. Eğer KOBİ risk seviyesi tüm profillerde "düşük" çıkmışsa "kontrol çerçeveleri", en az bir tane "orta" çıkmışsa "kontrol ve program çerçeveleri", en az bir tane "yüksek" çıkmışsa "kontrol, program ve risk çerçeveleri" uygulanabilir. Buradaki amaç KOBİ'lerin zaten kısıtlı olan işgücü ve gelirlerinin maliyet/etkin şekilde kullanılmasıdır.

8. SONUÇ VE ÖNERİLER

Türkiye İstatistik Kurumu "2018 yılı Girişimlerde Bilişim Teknolojileri Kullanım Araştırmasına" göre İnternet erişimine sahip girişimlerin oranı %95,3 olarak belirlenmiştir. Araştırma sonuçlarına göre 10 ve daha fazla çalışanı olan girişimlerin İnternete erişim oranı %95,3, 10-49 çalışanı olan girişimlerde %94,7, 50-249 çalışanı olan girişimlerde ise %97,8 olarak tespit edilmiştir. Yine aynı araştırmaya göre 10 ve daha fazla çalışanı olan girişimlerin %11,6'sı, çalışan sayısı 10-49 olan girişimlerin %8,2'si, 50-249 çalışanı olan girişimlerin %24,3'ü ana işi bilişim teknolojileri olan ve bilişim sistemleri ve uygulamalarının kurulması, işletilmesi ve geliştirilmesi süreçlerinde görev alan bilişim uzmanı istihdam etmiştir. Bu araştırma bize Türkiye'de KOBİ'lerin yoğun olarak bilgi ve iletişim teknolojisi kullanmalarına karşın yeterli uzman personel istihdam etmediklerini ve kaynak ayırmadıklarını göstermektedir.

Bu çalışmada bilgi güvenliği konusunda risk altında olduğu düşünülen KOBİ'ler için kendi kendilerine basit bir metotla risk profillerinin çıkarılması ve risk profiline uygun nasıl bir bilgi güvenliği stratejisi izlenmesi gerektiğine dair bir yol haritası çıkarılmaya çalışılmıştır.

KOBİ'ler her şeyden önce bilgi güvenliği risklerinin küçük büyük fark etmeden tüm işletmeleri tehdit ettiği gerçeğinin ve bilgi güvenliğinin işletmelerde yalnızca bilgi işlem çalışanlarının değil tüm çalışanların sorumluluğunun olduğunun farkında olmalıdırlar.

KOBİ'ler yaşadığımız bilgi çağının bir gereği olarak bilişim uzmanı istihdam etmeli, bunu bir mali külfet olarak görmemelidirler.

KOBİ'ler kendilerine soracakları birkaç basit soruyla risk profillerini çıkarabilirler. Risk profillerine uygun bir çerçeve uygulayarak maliyet-etkin bir bilgi güvenliği sistemi kurarak yalın ve aynı zamanda basit bir metodoloji izleyebilirler.

Risk profilinin tespit edilmesindeki özellikler ihtiyaca göre genişletilebilir veya azaltılabilir. Gelir ve BT kaynaklarına erişime ilişkin risk profilinin belirlenmesinde Türkiye'de KOBİ tanımının yapılmasında kullanılan nicel özelliklerden faydalanılmıştır.

Günümüzde bilgi artık işletmelerin en kıymetli varlıkları haline gelmiştir ve korunması gerekmektedir. Bilgi korunmadığı takdirde kötü niyetli kişilerin eline geçmesi kaçınılmazdır ve bu durumda işletme varlığını tehdit eden risklerle karşı karşıya kalınabilir.

9. Kaynakça

Abbas, J., Mahmood, K. H., & Hussain, F. (2015). INFORMATION SECURITY MANAGEMENT FOR SMALL AND MEDIUM SIZE ENTERPRISES. *Science International (Lahore)*, 2393-2398.

Alberts, C., & Dorofee, A. (2002). *Managing Information Security Risks: The OCTAVE Approach.* . Boston: Addison-Wesley.

Al-Safwani, N., Hassan, S., & Katuk, N. (2014). A Multiple Attribute Decision Making for Improving Information Security Control Assessment. *International Journal of Computer Applications, 89*(3), 19-24.

Amrin, N. (2014). *The Impact of Cyber Security on SMEs.* Twente: University of Twente, Electrical Engineering, Mathematics and Computer Science. Ekim 9, 2018 tarihinde https://essay.utwente.nl/65851/1/Amrin_MA_EEMCS.pdf adresinden alındı

ASQ. (tarih yok). *WHAT IS THE PLAN-DO-CHECK-ACT (PDCA) CYCLE?* Ağustos 12, 2018 tarihinde https://asq.org: https://asq.org/quality-resources/pdca-cycle adresinden alındı

Caralli , R., Stevens , J., Young , L., & Wilson , W. (2007). *Introducing OCTAVE Allegro:Improving the Information Security Risk Assessment Process.* Hanscom: SEI Administrative Agent.

Central Computer and Telecommunication Agency. (2009). *Risk Analysis and Management Method, Issue 2.0. CRAMM User Guide.* UK Central Computer and Telecommunication Agency.

Chang, S. E., & Ho, C. B. (2006). Organizational factors to the effectiveness of implementing information security management. *Industrial Management & Data Systems*(106), 345–361.

Cohen, J. K. (2017). *Health Information Technology*. www.beckershospitalreview.com: https://www.beckershospitalreview.com/healthcare-information-technology/ adresinden alındı

Dunkerley, K. D., & Tejay, G. (2011). A confirmatory analysis of information systems security success factors. *2011 44th Hawaii International Conference on System Sciences*, (s. 1–10). Honolulu, Hawaii.

Ein-Dor, P., & Segev, E. (1978). Organizational context and the success of management information systems. *Manage Sci.*(24), 1064–1077.

Ersoy, E. V. (2012). *ISO/IEC 27001 Bilgi Güvenliği Standardı.* Ankara: ODTÜ Yayıncılık.

European Network and Information Security Agency. (tarih yok). *CRAMM*. Temmuz 29, 2018 tarihinde www.enisa.europa.eu: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_cramm.html adresinden alındı

FAIR Institute. (tarih yok). Mart 09, 2019 tarihinde https://www.fairinstitute.org/what-is-fair adresinden alındı

Gordas, V. (2014). *Implementing Information Security Management System in SMEs and ensuring Effectiveness in its Governance.* Egham: University of London.

Guttman, B., & Roback, E. A. (1995). *Special Publication 800– 12. An introduction to computer security: the NIST handbook.* Gaithersburg, MD: NIST.

Hanacek, N. (2018). *Helping organizations to better understand and improve their management of cybersecurity ris*. NIST web Sitesi: https://www.nist.gov/cyberframework/online-learning/five-functions adresinden alındı

Hanseth, O., & Ciborra, C. (2007). *Risk, complexity and ICT.* Cheltenham, İngiltere: Edward Elgar Publishing.

Harris, K. D. (2016). *California Data Breach Report 2012-2015.* Kaliforniya: California Department of Justice.

Haythorn, M. (2015). *Running Head: Information Security Risk Assessment Methods, Frameworks and Guidelines.* East Carolina: East Carolina University. Eylül 15, 2018 tarihinde https://infosecwriters.com/Papers/MHaythorn_Risk_Frameworks_guidelines.pdf adresinden alındı

Hiscos. (2018). *2018 HISCOX Small Business Cyber Risk Report.* Kasım 15, 2018 tarihinde https://www.hiscox.com/documents/2018-Hiscox-Small-Business-Cyber-Risk-Report.pdf adresinden alındı

Houmb, S. H. (2007). *Decision Support for Choice of Security Solution: The Aspect-Oriented Risk Driven Development (AORDD) Framework.* Trondheim: Norwegian University of Science and Technology.

Ionita, D., Hartel, P., Pieters, W., & Wieringa, R. (2013). *Current Established Risk Assessment Methodologies and Tools.* Twente: University of Twente. doi:10.13140/RG.2.2.22914.68806

ISSA (Information Systems Security association). (2011, Mart). *ISSA-UK 5173 Information Security for Small and Medium Sized Enterprises*. https://issa.org: https://issa.org.pl/63-issa-uk-draft-standard-on-information-security-for-smes/file adresinden alındı

Jansen, W., & Scarfone, K. (2008). *Guidelines on Cell Phonand PDA Security, Recommendations of NIST. NIST Special Publication 800-124.* Gaithersburg: NIST.

Kankanhalli, A., Teo, H.-H., Tan, B., & Wei, K.-K. (2003). An integrative study of information systems security effectiveness. *The International Journal of Information Management*(23), 139-154.

Kirkpatrickprice. (2019). *What is HITRUST?* . https://kirkpatrickprice.com: https://kirkpatrickprice.com/hitrust/ adresinden alındı

Kotulic, A. G., & Clarck, J. (2004). Why there aren't more information security research studies. *Information & Management*(41), 597-607.

Kraemer, S., Carayon, P., & Clem, J. (2009). Human and organizational factors in computer and information security: pathways to vulnerabilities. *Computer & Security*(28), 509-520.

Lacey, D., & James, B. (2010, Mart). *Review of Availability of Advice on Security for Small/Medium Sized Organisations*. Information Commissioner's Office: https://ico.org.uk/media/about-the-ico/documents/1042344/review-availablility-of-security-advice-for-sme.pdf adresinden alındı

Lord, N. (2018, September 11). *Datainsider*. https://digitalguardian.com: https://digitalguardian.com/blog/what-nist-sp-800-53-definition-and-tips-nist-sp-800-53-compliance adresinden alındı

Manso, C. G., Rekleitis, E., Papazafeiropoulos, F., & Maritsas, V. (2015). *Information security and privacy standards for SMEs.* European Union Agency for Network and Information Security (ENISA). doi:10.2824/829076

Marttin, V., & Pehlivan, İ. (2010). ISO 27001:2005 Bilgi Güvenliği Yönetimi Standardı ve Türkiye'deki Bazı Kamu Kuruluşu Uygulamaları Üzerine Bir inceleme. *Mühendislik Bilimleri ve Tasarım Dergisi, 1*(1), 49-56.

Mayer, N. (2009). *Overview of CRAMM*. Kasım 22, 2018 tarihinde www.researchgate.net: https://www.researchgate.net/figure/Overview-of-CRAMM-as-appears-in-cra_fig5_30512823 adresinden alındı

Mijnhardt , F., Thijs , B., & Spruit, M. (2016). Organizational Characteristics Influencing SME Information Security Maturity. *Journal of Computer Information Systems, 56*(2), 106-115.

Miller, G. (2017). *60% of small companies that suffer a cyber attack are out of business within six months.* Aralık 20, 2018 tarihinde The Denver Post: https://www.denverpost.com/2016/10/23/small-companies-cyber-attack-out-of-business/ adresinden alındı

NIST. (2012). Information Security. *Guide for Conducting Risk Assesments*, s. 2. https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf adresinden alındı

NIST. (2016, Ağustos 25). *Cybersecurity Framework FAQS Framework Basics*. Aralık 24, 2018 tarihinde NIST Web Sitesi: https://www.nist.gov/cyberframework/cybersecurity-framework-faqs-framework-basics adresinden alındı

NSBA. (2013). *2013 SMALL BUSINESS TECHNOLOGY SURVEY*. Mart 2019, 07 tarihinde National Small Bussiness Associaton: https://www.nsba.biz/wp-content/uploads/2013/09/Technology-Survey-2013.pdf adresinden alındı

Öztürk, G. (2008). *Bilgi Güvenliği Politikası Oluşturma Kılavuzu Doküman Kodu: BGYS-0005.* Kocaeli: TÜBİTAK.

Park, J.-Y., Robles, J. R., Hong, C.-H., & Yeo, S.-S. (2008, Ocak). IT Security Strategies for SME's. *International Journal of Software Engineering and its Applications, 2*(3), 91-98.

Pironti, J. P. (2013). Key Elements of an Information Risk Profile. *ISACA JOURNA*(4), 1-5.

Rapid7. (tarih yok). *CIS Critical Security Controls*. www.rapid7.com/: https://www.rapid7.com/fundamentals/cis-critical-security-controls/ adresinden alındı

Rehage, K., Hunt , S., & Nikitin, F. (2008). *Global technology audit guide: developing the IT audit plan.* ABD: Altamonto Springs.

Risk Management Insight LLC. (2006). *FAIR (Factor Analysıs Of Informatıon Rısk) Basic Risk Assessment Guide.* ABD: Risk Management Insight LLC.

SANS. (2018). *CIS Controls.* Haziran 21, 2018 tarihinde Poster4_CIS-Security-Controls_2018.indd: https://www.sans.org/security-resources/posters/security-leadership-cis-controls/55/download adresinden alındı

Sean , M. B., Ahmad, A., & Ng, Z. (2013). Information Security Management: Factors That Influence Security Investments in SMEs. *11th Australian Information Security Management Conference.* Churchlands: Australia:Edith Cowan University.

Secure Shell. (2018). *NIST CYBERSECURITY FRAMEWORK*. www.ssh.com: https://www.ssh.com/compliance/cybersecurity-framework/#sec-Overview-of-the-NIST-Cybersecurity-Framework adresinden alındı

Shanthamurthy, D. (2011, Ağustos). *NIST SP 800-30 standard for technical risk assessment: An evaluation.* Computerweekly.com: https://www.computerweekly.com/tip/NIST-SP-800-30-standard-for-technical-risk-assessment-An-evaluation adresinden alındı

Smith, S., & Jamieson, R. (2006). Determining Key Factors in E-Government Information System Security. *Information Systems Management, 23*(2), 23-32.

Soomro , Z. A., Shah, M. H., & Ahmed, J. (2016). Information security management needs more holistic approach: A literatüre review. *International Journal of Information Management, 36*(2), 215-225.

Stoneburner, G., Goguen, A., & Feringa, A. (2002). *SP800-30 Risk Management Guide for Information Technology Systems.* Gaithersburg: NIST. Temmuz 27, 2018 tarihinde Threat and Risk Management: https://www.enisa.europa.eu/topics/threat-risk-management/risk-management/current-risk/risk-management-inventory/rm-ra-methods/m_sp800_30.html adresinden alındı

Tawileh, A., Hilton , J., & McIntosh, S. (2007). Managing Information Security in Small and Medium Sized Enterprises: A Holistic Approach. *ISSE/SECURE 2007 Securing Electronic Business Processes*, 331-339.

Tewari, A. (2019). *Comparison between ISO 27005, OCTAVE & NIST SP 800-30*. Mart 2019 tarihinde https://www.sisainfosec.com/blogs/comparison-between-iso-27005-octave-nist-sp-800-30/ adresinden alındı

The Open Group. (2009). *Technical Standard Risk Taxonomy.* Berkshire: The Open Group. Eylül 15, 2018 tarihinde http://pubs.opengroup.org/onlinepubs/9699919899/toc.pdf adresinden alındı

TS ISO/IEC 27002. (2013). *Bilgi Güvenliği - Güvenlik Teknikleri - Bilgi Güvenliği Kontrolleri İçin Uygulama Prensipleri.* ISO/IEC.

Whitman, M., & Mattford, H. (2011). *Principles of information security* (4 b.). İngiltere: Cengage Learning.

Zaras, D. (2018). *Information Security Frameworks and Controls Catalogs.* ABD: Impactmakers.

Research Article

Küçük ve Orta Büyüklükteki İşletmelerde Bilgi Güvenliği

Information Security in Small And Medium Size Companies

Murat Sami BAYKIZ	Cihan TANRIÖVEN
İç Denetçi, Gazi Üniversitesi, Bilişim Enstitüsü, Yönetim Bilişim Sistemleri mbaykiz@gmail.com https://orcid.org/0000-0001-9129-3619	Prof. Dr. Ankara Hacı Bayram Veli Üniversitesi, İktisadi ve İdari Bilimler Fakültesi İşletme Bölümü cihantt@gmail.com https://orcid.org/0000-0003-0192-7628

EXTENSIVE SUMMARY

Especially in the late 20th century, the ways in which the development of information and communication technologies were applied to business processes rapidly changed the way businesses work. While this process of change was an opportunity for some enterprises, it led to risks and crises for some enterprises.

Large companies are trying to take the necessary measures by employing adequate professional labor and allocating budget, for risks related to information security. SMEs who do not invest in information security and who refrain from employing a sufficient number of information technology personnel due to costs are unable to take the necessary measures and SMEs become easy targets against abuses and cybercriminals.

In a study it has been determined that 47% of SMEs are exposed to information security attacks in 2017 at least once. In another study conducted again; it is stated that 60% of the SMEs that are exposed to attacks terminate their activities within six months.

Information security risks threaten all business types, including SMEs. The implementation of standards on information security is very important for taking measures before they occur and mitigating risk impacts. Taking measures to ensure information security and presenting this phenomenon to the stakeholders is the reason for giving added value to SMEs and being preferred. Many national and international legislation compel enterprises to take measures related to information security, including SMEs.

There are some obstacles to SMEs' adoption of information security. SMEs are not aware of the information security standards. The standards that SMEs can use are limited and there are generally no standards that take into account the characteristics of the sector in which they work. SME managers are not aware of the added value that information security standards provide to their businesses. Many SME executives see large companies as targets for cyber attacks, and they do not believe that these attacks are targeted their SME's. SMEs face difficulties in establishing an effective and efficient information security control due to resource constraints and insufficient knowledge. There are many complex standards for information security. These standards require expertise and are designed to meet the needs of large enterprises.

There are many approaches in the context of measures to be taken regarding information security. The first category of these approaches are control frameworks. Control frames define the security controls that are the basis of each security program. Here is some examples for control frames:

- Center for Internet Security Controls, CIS CSC
- NIST Special Publication (SP) 800-53
- ISO/IEC 27002 (Information technology - Security techniques - Code of practice for information security controls)

The second category, program frameworks, helps to configure the security program, provide a basis for evaluating program activities, and simplifies communication about the program. Here is some examples for program frames:

- HITRUST Cybersecurity Framework
- NIST Cybersecurıty Framework
- ISO/IEC 27001 (Information technology - Security techniques - Information security management systems - Requirements)

Risk frameworks offer a coherent approach to managing and evaluating risk in a way that is valuable to the business. And some risk frameworks are:

- ISO 27005 (Information Technology - Security Techniques - Information Security Risk Management)
- NIST SP800-30 (Risk Management Guide for Information TechnologySystems)
- FAİR-Factor Analysis of Information Risk
- OCTAVE-Operationally Critical Threat, AssetandVulnerability Evaluation

While control frameworks require little time and little experience, the application of risk frameworks is more complex and requires much time and expertise. More time and expertise also means cost.

The information risk profile is critical to the success of an enterprise's information risk management strategy and operations. Provides valuable information about an enterprise's information risk appetite and information risk management expectations, and provides important clues for risk management for decision makers. The SME characteristics that can be utilized in the risk profile of SMEs are: obligations of the legislation (such as using or not using personal data), information confidentiality, integrity, accessibility, operating income / gain, number of employees, and dependency on information systems.

It is possible to divide the risk levels into three in the qualitative evaluation method used in the information security risk assessment. These;

• *High* - Significant material impact on loss of customer confidence, loss of brand reputation, assets, critical business processes and / or business operations

• *Medium* - Financial impact on customer loss of trust, loss of brand reputation, assets, critical business processes and / or business operations,

• *Low* - Minimal material impact on assets, critical business processes and / or business operations, a minor change in customer trust and / or brand reputation.

Profiles determined according to SME characteristics can be divided into high, medium and low risk levels used in the qualitative evaluation method. Here is an example of risk profile related to dependency on information systems;

Table- Risk profile for the degree of tolerance to IT interruptions

1	I lose customers / stop operations as soon as there is an IT outage.	High
2	If the IT interruption lasts more than 24 hours, I lose my customers / my operations will stop.	Middle
3	If the IT outage lasts more than 24 hours, I lose my customers / my operations will stop.	Low

Once a risk profile has been identified in an SME, the appropriate framework can be selected according to the risk level. If the SME risk level is “low” in all profiles, control frames; control and program frames if at least one “medium” is present; control, program and risk frames can be applied if at least one “high” is available. Various risk profiles of other features of SMEs can be

created. These risk profiles are graded to select the appropriate information security framework and measures can be taken against risks. In this approach, the objective is to use the limited workforce and income of SMEs in a the cost / efficiency way.

In this study, a road map was prepared for SMEs that are considered to be at risk in terms of information security, by using a simple method to obtain risk profiles and how to follow an information security strategy for risk profile. SMEs can take risk profiles with a few simple questions to ask themselves. Implementing a cost-effective information security system by applying a framework that is appropriate to risk profiles, they can follow a simple methodology.

SMEs should be aware that the risks of information security threaten all businesses without little notice, and that information security is the responsibility of all employees, not just the IT staff. SMEs should employ informatics experts as a requirement of the information age, and should not see this as a financial burden.

Nowadays, knowledge has become the most valuable assets of enterprises and needs to be protected. If the information is not protected, it is inevitable for malicious persons to be seized and in this case, the risks that threaten the existence of the enterprise may be faced.