Co-funded by the
Erasmus+ Programme
of the European Union

InCyT Eğitim Modülü

Yöneticiler için Bilgi Güvenliği Ünite (Modül) 4, Hafta 7 ve 8 Birim (Modül) adı: Siber Risk ve Esneklik	
Öğrenme Aktiviteleri	❑ **Web Semineri**❑ **Alıştırmaları**❑ **Atölye Sunumu**❑ **Diğer**
Öğrenme Sorumlusu	• Simon Tjoa • Peter Kieseberg
Öğrenme Etkinliği Hedefleri	1. Katılımcılar risk ve dayanıklılık yönetiminin temellerini bilirler 2. Katılımcılar iş etki analizi ve risk analizi yapabileceklerdir. 3. Katılımcılar karşı önlemleri ve güvenlik kararlarını analiz sonuçlarından türetebilirler.
Kazanılacak Beceriler	• 1'DIR, 3'TÜR. • MS 1
Öğrenme aktivitesinin süresi	2 hafta • 7. Hafta (2 saat) • 8. Hafta (2 saat)
Öğrenme rdonatımları	***Neye ihtiyaç var?*** • Temel yönetim becerileri • Temel BT becerileri • Temel güvenlik becerileri

Co-funded by the
Erasmus+ Programme
of the European Union

Modül hakkında kısa bilgi

Giriş
Mükemmel güvenlik mümkün değildir. Bunu bilerek, doğru güvenlik önlemleri için nasıl para harcanacağına dair bilinçli kararlar vermek hayati önem taşımaktadır. Siber risk ve esneklik yönetimi, bir kuruluşun mevcut güvenlik durumunu değerlendirmek ve bilgi güvenliği riskini kabul edilebilir bir seviyede tutmak için kontrolleri planlamak için hayati bir araç ve teknik seti sağlar.

Öğrenme Materyalinin İçeriği

Risk almadan, iş yapmak imkansızdır. Bu nedenle, risk yönetimi ve ilgili araçlar ve teknikler, riski ele almak için sistematik bir yol sağlar. Ne kadar güvenliğin yeterli olduğu veya öncelikle hangi karşı önlemin uygulanması gerektiği gibi sorular risk yönetimi tarafından cevaplandırılmaktadır. Bu nedenle, risk yönetimi, bilinçli kararlar alınmasını sağlamak için önemli bir faaliyettir. Bu temel konuyu ele alan önemli standartlar ve en iyi uygulamalar arasında ISO 27005, ISO 31000 veya BSI 200-3 bulunmaktadır.

Risk yönetimi sürecine daha yakından bakmadan önce, temel terimleri tanımlamak önemlidir:

- **Güvenlik açığı:** "Bir bilgi sisteminde, sistem güvenlik prosedürlerinde, iç denetimlerde veya uygulamada bir tehdit kaynağı tarafından istismar edilebilecek veya tetiklenebilecek zayıflık."[1]
- **Kontrol:** "Bir bilgi sistemi veya bir kuruluş için, bilgilerinin gizliliğini, bütünlüğünü ve kullanılabilirliğini korumak ve tanımlanmış bir dizi güvenlik gereksinimini karşılamak için tasarlanmış bir koruma veya karşı önlem."[2]
- **Tehdit:** "Örgütsel operasyonları (misyon, işlevler, imaj veya itibar dahil), örgütsel varlıkları, bireyleri, diğer kuruluşları veya Ulusu, yetkisiz erişim, imha, ifşa, bilginin değiştirilmesi ve / veya hizmet reddi yoluyla bir bilgi sistemi aracılığıyla olumsuz etkileme potansiyeline sahip herhangi bir durum veya olay."[3]
- Risk: "Bir işletmenin potansiyel bir durum veya olay tarafından ne ölçüde tehdit edildiğinin bir ölçüsüdür ve tipik olarak şunların bir fonksiyonudur: (i) durum veya olayın meydana

[1] https://csrc.nist.gov/glossary/term/vulnerability
[2] https://csrc.nist.gov/glossary/term/security_control
[3] https://csrc.nist.gov/glossary/term/threat

gelmesi durumunda ortaya çıkacak olumsuz etki veya zararın büyüklüğü; ve (ii) oluşma olasılığı."[4]

"belirsizliğin hedefler üzerindeki etkisi"[5]

ISO 31000 ("belirsizliğin etkisi") tanımından, risklerin olumlu ve olumsuz etkileri olabileceğini söyleyebiliriz. Genellikle risklerin olumlu etkileri varsa, fırsatlar olarak adlandırılırlar.

Genel risk yönetimi süreci kapsam, bağlam ve kriterler ile başlar. Tüm faaliyetler için tüm riskler analiz edilemediğinden, hangi hizmetlerin, süreçlerin ve organizasyon birimlerinin değerlendirmeye dahil edilmesi gerektiğine öncelik vermek ve karar vermek önemlidir. Yeterli bir kapsama sahip olmak, bir yandan geçerli sonuçlar ve diğer yandan makul çaba sağlamak için çok önemlidir. Bağlam, iç ve dış ortamdır. Risk kriterlerinin belirlenmesi, karşılaştırılabilir sonuçlara yol açan tekrarlanabilir bir süreç sağlamak için önemlidir. Kriterler, farklı kişilerin riskleri ortak bir şekilde değerlendirebilecekleri şekilde tanımlanmalıdır.

Kriterlere örnek olarak, finansal, itibar veya sağlık gibi çeşitli boyutlar için etki kriterleri (ör. düşük, orta, yüksek) verilebilir.

Aşağıda, OCTAVE Allegro'nun itibar ve müşteri etkileri ile ilgili bir örneği sunulmuştur:

Allegro Worksheet 1	RISK MEASUREMENT CRITERIA – REPUTATION AND CUSTOMER CONFIDENCE		
Impact Area	Low	Moderate	High
Reputation	Reputation is minimally affected; little or no effort or expense is required to recover.	Reputation is damaged, and some effort and expense is required to recover.	Reputation is irrevocably destroyed or damaged.
Customer Loss	Less than _____% reduction in customers due to loss of confidence	_____to _____% reduction in customers due to loss of confidence	More than _____% reduction in customers due to loss of confidence
Other:			

Şekil 1: İtibar için Ölçüm Kriterleri[6]

Risk kriterlerinin ve kapsamının tanımlanmasından sonra ilk adım risklerin belirlenmesidir. Risk tanımlama, yalnızca tanımlanan risklerin değerlendirilebileceği için çok önemlidir. Bu nedenle, tanımlanan tehditleri ISO 27005, MEHARI veya diğer en iyi uygulamalar veya standartların tehdit listeleriyle karşılaştırmak mantıklıdır.

[4] https://csrc.nist.gov/glossary/term/risk
[5] https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
[6] https://resources.sei.cmu.edu/asset_files/technicalreport/2007_005_001_14885.pdf

Beyin fırtınası, Delphi tekniği, Hata Modu ve Etki Analizi (FMEA) veya Tehlike ve İşletilebilirlik çalışmaları (HAZOP) gibi riskleri tanımlamak için çeşitli teknikler vardır.[7]

Bir sonraki adım risk analizinde, belirlenen risklerin daha iyi anlaşılması sağlanır. Bu nedenle, oluşum olasılığı/sıklığı ve etki/sonuçları belirlenir. Sonuçları belirlemek için, etkilerin nasıl değerlendirildiğini sistematik bir şekilde tanımlamak önemlidir. Genellikle nitel bir ölçünün (örneğin, düşük, orta, yüksek) kullanımı nicel ölçümlerden daha kolaydır.

Riskler genellikle, olasılık ve etkiyi eksen olarak kullanarak riski vurgulayan bir risk matrisinde görselleştirilir.

Probability	Harm severity			
	Minor	Marginal	Critical	Catastrophic
Certain	High	High	Very high	Very high
Likely	Medium	High	High	Very high
Possible	Low	Medium	High	Very high
Unlikely	Low	Medium	Medium	High
Rare	Low	Low	Medium	Medium
Eliminated	Eliminated			

Şekil 2: Risk Matrisi [Kaynak Vikipedi][8]

Bir sonraki adımda, riskler değerlendirilir. Bu, önceki adımın sonuçlarının, eylemlerin yapılması gerekip gerekmediğine karar vermek için dikkate alındığı anlamına gelir. Ayrıca, risklerin önceliklendirilmesi gerçekleşir.

Riskleri ele almak için dört ana stratejiden biri belirlenir:

- Risk kabulü: Riskin kuruluşun risk iştahı içinde olup olmadığını belgelemek ve izlemek
- Risk transferi: Hisse riskleri (örneğin, sigorta, ortak girişim)
- Riskten kaçınma: Risk kaynağını ortadan kaldırın (örneğin, hava boşluğu)
- Risk azaltma: Etki veya oluşum olasılığını azaltın (örneğin, erişim kontrolü)

Önlemlerin belirlenmesinden sonra, artık riskin kabul edilebilir olup olmadığı veya daha fazla önlem alınması gerekip gerekmediği değerlendirilir.

[7] cesaret. https://www.iso.org/standard/72140.html
[8] https://en.wikipedia.org/wiki/Risk_matrix

Ana risk değerlendirme sürecinin yanı sıra destekleyici faaliyetler olarak, risk iletişimi (yani ilgili paydaşla iletişim), risk izleme ve risk raporlama gerçekleşir.

Tüm riskler dikkate alınamayacağından, risk yönetiminin aksine, iş sürekliliği ve esnekliği bireysel riskler yerine kritik faaliyetlere odaklanır. Bu şekilde bilinmeyen ve düşük olasılıklı/yüksek etkili risklere hazırlanmak mümkündür.

Etkin bir iş sürekliliği programının sağlanması için üst yönetimin desteği hayati önem taşımaktadır. İş sürekliliği yönetiminin önemini vurgulayan önemli bir eser, iş sürekliliği politikasıdır. Bu belgede yönetim katılımı resmi olarak ifade edilmiştir. Ayrıca, belge, iş sürekliliği faaliyetlerinin kapsamını ve amaçlarını, önemli rol ve sorumlulukları (örneğin, iş sürekliliği yöneticisi) ve programın gerçekleştirilmesi için kullanılan operasyonel çerçeveyi vurgulamaktadır. Analizin karmaşıklığının ve çabanın çok fazla yükselmemesini sağlamak için kapsamın çok geniş olmaması gerektiği vurgulanmalıdır.

Hizmet kesintilerinin işletme üzerindeki etkilerini anlamak ve kurtarma önlemlerini planlamak için iyi bir temele sahip olmak amacıyla, iş etki analizleri yapılmaktadır. İş sürekliliği sürecindeki merkezi araçtır ve ürünlerin/hizmetlerin alaka düzeyini/önemini yakalar. Ürün / hizmetlerin kritikliği dışında, bağımlılıkları belirlenir ve değerlendirilir.

Bir iş etki analizi yaparken kullanılan önemli anahtar rakamlar şunlardır:

- **MAO (maksimum kabul edilebilir kesinti): "Bir** ürün / hizmet sağlamamanın veya bir faaliyette bulunmamanın bir sonucu olarak ortaya çıkabilecek olumsuz etkilerin [...] kabul edilemez hale gelmesi için gereken süre [...]"[9]
- **RTO (kurtarma süresi hedefi):** "Bir olayı takip eden süre [...] içinde bir ürün ve hizmetin [...] veya bir faaliyetin [...] devam ettirildiği veya kaynakların [...] geri kazanıldığı "[10]
- **RPO (kurtarma noktası hedefi):** "hangi bilgilere işaret eder [...] bir etkinlik tarafından kullanılan [...] etkinliğin yeniden başlatıldığında çalışmasını sağlamak için geri yüklenir"[11]

İlk adımda, en kritik veya temel ürün ve hizmetler belirlenir. Tanımlamadan sonra, belirli bir ürün veya hizmetin kesintiye uğraması veya kesintiye uğraması durumunda zaman içinde hangi hasarın ortaya çıkacağı değerlendirilir.

Başarılı olan şekil, zaman içindeki etkinin bir elektronik tabloda nasıl yakalanabileceğini göstermektedir.

[9] MAO https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[10] RTO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en
[11] RPO, https://www.iso.org/obp/ui#iso:std:iso:22300:ed-3:v1:en

Assessment Period / Damage Category	1 Hour(s)	2 Hour(s)	4 Hour(s)	8 Hour(s)	24 Hour(s)	48 Hour(s)	96 Hour(s)	168 Hour(s)	240 Hour(s)	720 Hour(s)
Financial	0	0	0	0	0	0	2	3	4	4
Health & Safety	0	0	0	0	0	0	0	3	4	4
Legal, Regulatory & Contractual	0	0	0	0	1	1	1	2	2	2
Brand and Reputation	0	0	0	1	1	1	2	4	4	4
Environmental	0	0	0	0	0	0	0	0	0	0
Rational for the assessment (Description) Verbal Description of Implications										

Ayrıca, ilgili hizmetlerle ilgili süreçlerin, faaliyetlerin ve kaynakların bağlı olduğu iş etki analizi anketleri de yer almaktadır. Bu şekilde, kurtarma süresi hedefi, kurtarma noktası hedefi ve kabul edilebilir maksimum kesinti gibi önemli önemli rakamlar belirlenebilir.

Süreçlerin, hizmetlerin ve kaynakların kritikliği bilindikten sonra iş sürekliliği stratejileri detaylandırılır. Stratejiler arasında diğerlerinin yanı sıra çeşitlendirme (örneğin, coğrafi olarak ayrılmış yerlerdeki etkinlikler), çoğaltma (örneğin, başka bir sitede kurtarmak için verileri kopyalama) veya taşeronluk (örneğin, üçüncü taraf hizmetlerini kullanma) bulunur.

Stratejilere dayanarak, kuruluşların bir olayın ardından verimli bir şekilde tepki vermelerini destekleyen iş sürekliliği planları yazılır. Yüksek basınçlı durumlarda kullanılabilmesi için planların buna göre yazılması hayati önem taşımaktadır. Bu, planların yalnızca bir olayı ele alırken ilgili olan bilgileri içermesi gerektiği anlamına gelir. Ayrıca, bilgilerin kavranması hızlı olmalıdır. Bu nedenle, açık ve eylem odaklı kontrol listeleri kullanılmalıdır.

Tipik iş sürekliliği planları amaç, kapsam, olay yönetimi yapısı, roller ve sorumluluklar, plan etkinleştirme, kurtarma düzenlemeleri ve iletişim ayrıntıları hakkında bilgiler içerir.

Planların yeterliliğini prova etmek ve kontrol etmek için farklı egzersiz türleri kullanılır. Bu, masa üstü kontrolleri veya masa başı alıştırmaları gibi tartışmaya dayalı alıştırmalar veya belirli sistemlerin geri yüklenmesini test etmek gibi teknik alıştırmalar olabilir.

Soru:

Word Belgelerine Bakın

Eks:

Powerpoint ve Video dosyalarına bakın

Başvuru:

- ISO 22301:2019, Güvenlik ve esneklik - İş sürekliliği yönetim sistemleri - Gereksinimler
- ISO 22313:2020, Güvenlik ve esneklik - İş sürekliliği yönetim sistemleri - ISO 22301'in kullanımına ilişkin kılavuz
- ISO/TS 22317:2021, Güvenlik ve esneklik - İş sürekliliği yönetim sistemleri - İş etki analizi için kılavuzlar
- ISO/TS 22331:2018, Güvenlik ve esneklik - İş sürekliliği yönetim sistemleri - İş sürekliliği stratejisi için kılavuzlar
- ISO/TS 22332:2021, Güvenlik ve esneklik - İş sürekliliği yönetim sistemleri - İş sürekliliği planları ve prosedürleri geliştirmek için kılavuzlar
- ISO 31000:2018, Risk yönetimi — Kılavuzlar, https://www.iso.org/obp/ui/#iso:std:iso:31000:ed-2:v1:en
- IEC 31010:2019, Risk yönetimi — Risk değerlendirme teknikleri