İŞLETME RİSKLERİNİN YÖNETİMİ VE SİGORTACILIK SİSTEMİNE DEVRİ

Ocak 2024

Yayın No: TÜSİAD-T/2024-01/635

Meşrutiyet Caddesi, No: 46 34420 Tepebaşı / İstanbul

Telefon: (0212) 249 07 23 Telefaks (0212) 249 13 50

www.tusiad.org

Kapak Tasarımı: İsmet Tosunoğlu

Dizgi ve Sayfa Uygulama: İsmet Tosunoğlu

ÖNSÖZ

TÜSİAD, özel sektörü temsil eden sanayici ve iş insanları tarafından 1971 yılında, Anayasamızın ve Dernekler Kanunu'nun ilgili hükümlerine uygun olarak kurulmuş, kamu yararına çalışan bir dernek olup gönüllü bir sivil toplum örgütüdür.

TÜSİAD, insan hakları evrensel ilkelerinin, düşünce, inanç ve girişim özgürlüklerinin, laik hukuk devletinin, katılımcı demokrasi anlayışının, liberal ekonominin, rekabetçi piyasa ekonomisinin kurum ve kurallarının ve sürdürülebilir çevre dengesinin benimsendiği bir toplumsal düzenin oluşmasına ve gelişmesine katkı sağlamayı amaçlar. TÜSİAD, Atatürk'ün öngördüğü hedef ve ilkeler doğrultusunda, Türkiye'nin çağdaş uygarlık düzeyini yakalama ve aşma anlayışı içinde, kadın-erkek eşitliğini siyaset, ekonomi ve eğitim açısından gözeten iş insanlarının toplumun öncü ve girişimci bir grubu olduğu inancıyla, yukarıda sunulan ana gayenin gerçekleştirilmesini sağlamak amacıyla çalışmalar gerçekleştirir.

TÜSİAD, kamu yararına çalışan Türk iş dünyasının temsil örgütü olarak, girişimcilerin evrensel iş ahlakı ilkelerine uygun faaliyet göstermesi yönünde çaba sarf eder; küreselleşme sürecinde Türk rekabet gücünün ve toplumsal refahın, istihdamın, verimliliğin, yenilikçilik kapasitesinin ve eğitimin kapsam ve kalitesinin sürekli artırılması yoluyla yükseltilmesini esas alır.

TÜSİAD, toplumsal barış ve uzlaşmanın sürdürüldüğü bir ortamda, ülkemizin ekonomik ve sosyal kalkınmasında bölgesel ve sektörel potansiyelleri en iyi şekilde değerlendirerek ulusal ekonomik politikaların oluşturulmasına katkıda bulunur. Türkiye'nin küresel rekabet düzeyinde tanıtımına katkıda

bulunur, Avrupa Birliği (AB) üyeliği sürecini desteklemek üzere uluslararası siyasal, ekonomik, sosyal ve kültürel ilişki, iletişim, temsil ve işbirliği ağlarının geliştirilmesi için çalışmalar yapar. Uluslararası entegrasyonu ve etkileşimi, bölgesel ve yerel gelişmeyi hızlandırmak için araştırma yapar, görüş oluşturur, projeler geliştirir ve bu kapsamda etkinlikler düzenler.

TÜSİAD, Türk iş dünyası adına, bu çerçevede oluşan görüş ve önerilerini Türkiye Büyük Millet Meclisi (TBMM)'ne, hükümete, diğer devletlere, uluslararası kuruluşlara ve kamuoyuna doğrudan ya da dolaylı olarak basın ve diğer araçlar aracılığı ile ileterek, yukarıdaki amaçlar doğrultusunda düşünce ve hareket birliği oluşturmayı hedefler.

TÜSİAD, misyonu doğrultusunda ve faaliyetleri çerçevesinde, ülke gündeminde bulunan konularla ilgili görüşlerini bilimsel çalışmalarla destekleyerek kamuoyuna duyurur ve bu görüşlerden hareketle kamuoyunda tartışma platformlarının oluşmasını sağlar.

TÜSİAD Ekonomi ve Finans Yuvarlak Masası'na bağlı Sigortacılık ve Bireysel Emeklilik Çalışma Grubu'nun faaliyetleri çerçevesinde yayınlanan "İşletme Risklerinin Yönetimi ve Sigortacılık Sistemine Devri" başlıklı bu rapor Çalışma Grubu Üyesi Kazım Murat Vargün'ün koordinasyonunda Çalışma Grubu üyeleri Anıl Gümüş, Batu Kan, Cem Öztürk, Ceyhun Eren, Ercan Erbek, Fatma Zerrin Caner, Ferit Erman, Gonca Ulusoy, Murat Eroğlu ve Savaş Yılmaz'ın katkılarıyla hazırlanmıştır.

İÇİNDEKİLER

1. **YÖNETİCİ ÖZETİ 9**

2. İŞLETME RİSKLERİ VE YÖNETİM STRATEJİLERİ 13

2.1. Temel Yangın Risklerinin Yönetimi 13

2.1.1. Genel Önlemler 14

2.1.2. Yanıcı ve Parlayıcı Kimyasallar Kullanan İş Yerlerinde Alınması Gereken Önlemler 17

2.1.3. İşletmelerde Depolama Standartları 19

2.1.4. Endüstriyel Tesislerde Çevresel Riskler 20

2.1.5. Bina Riskleri 20

2.2. Kriz Yönetimi 21

2.3. Olay Yönetimi 27

2.4. Bilgi Güvenliği Riskleri ve Yönetimi 30

2.5. Bilgi Teknolojileri Hizmet Süreklilik Riski ve Yönetimi 34

2.6. Tedarikçi Riskleri ve Yönetimi 39

3. İŞLETME RİSKLERİNİN SİGORTACILIK VASITASIYLA DEVRİ 47

3.1. Doğru Sigorta Aracısı Seçimi 48

3.2. Sigortalanabilir Varlıkların Belirlenmesi ve Envanteri 49

3.3. Doğru Ürün ve Teminatların Belirlenmesi 50

3.4. Sigorta Fiyatlamasına Etki Eden Faktörler 56

3.5. Doğru Teminat Bedellerinin Belirlenmesi ve Eksik/Aşkın Sigorta 57

3.6. Sigorta Şirketleri ile Hasar Yönetimi 60

BÖLÜM 1

YÖNETİCİ ÖZETİ

1. YÖNETİCİ ÖZETİ

2023 yılı başında yaşanan büyük deprem felaketi, hepimizi yasa boğarken ülkemizde ve dünyada yaşanan doğal afetlerin ne kadar yıkıcı olabileceğini bir kez daha hatırlatmıştır. Bu tür olaylar geri getirilemeyecek can kayıpları yanında, aynı zamanda işletmelerin ve hane halkının ekonomik açıdan da derin yaralar almasına neden olmaktadır. Bu bağlamda, sigortacılığın ve işletmelerin risk yönetiminin önemi daha da belirgin hale gelmektedir.

Bu nedenle, bu rapor, işletmelerin daha iyi bir risk yönetimi stratejisi oluşturmalarına rehberlik etmeyi ve toplumun genel direncini artırmayı hedeflemektedir. Bu çerçevede, raporun içeriği, işletmelerin karşılaşabileceği çeşitli riskleri değerlendirmek ve bu risklere karşı etkili bir şekilde korunma sağlamak için uygulanabilir stratejiler sunmaktadır. İşletmelerin bu stratejilere odaklanarak, sadece kendi dayanıklılıklarını artırmakla kalmayacak, aynı zamanda toplumun genel direncine de katkıda bulunacaklarına inanıyoruz.

Günümüzde tüm kurumlar doğal afetlerin yanında; operasyonel, makroekonomik, fiziki riskler başta olmak üzere bilgi güvenliği ve bilgi sistemlerinin sürekliliği riskleri, tedarikçi riskleri gibi çok çeşitli risklerle çevrelenmiştir. Riskleri etkili bir şekilde yönetemeyen kurumlar, finansal kayıplardan itibar kaybına, operasyonel aksamalara, hukuki sorunlara, iş ortakları ve paydaşlarıyla uyuşmazlıklara kadar bir dizi olumsuz sonuçla karşılaşabilir. Hatta, bu olumsuz etkiler işletmenin devamlılığını da tehdit edebilir.

Yukarıda bahsi geçen geleneksel risklerin yanında, işletmelerin orta vadede önlem alması gereken yükselen riskler de mevcuttur. Bunlar arasında, jeopolitik riskler, dijital dezenformasyon, bulaşıcı hastalıklar, anti-mikrobiyal direnç, yapay zekâ, mevzuat riskleri, beceri eksikliği ve yeniden istihdam zorluğu gibi riskler sayılabilir.

Risk yönetiminde birinci basamak olarak adlandırılan ve işletme bünyesinde kurulacak risk yönetimi sürecinin, kurumların hedeflerine ulaşmasında ve devamlılıklarında en az sigorta çözümleri kadar etkili olduğu bilinmektedir.

Bu raporun birinci bölümü işletmelerin kendi bünyelerinde risklerini doğru yönetebilmelerine rehber olması amacıyla hazırlanmıştır. Bu kapsamda risk yönetimi süreçlerinin temel adımlarını her bir risk özelinde tanımlamaktadır. Aynı zamanda, Dünya genelinde ve ülkemizde kabul görmüş çeşitli standartlara atıfta bulunmakta ve işletmelerin birinci basamak risk yönetimi süreçlerini uygulamaya koymalarına rehberlik etmesi amacıyla yönetişim modellerini detaylı bir şekilde tanıtmaktadır. Öte yandan ilk bölümde olay/hasar öncesi riski azaltma/önleme çalışmalarında risk mühendisliği kavramını açıklamaktadır.

İkinci bölümde ise riskin devredilmesi (sigorta) kavramı incelenmiş olup, doğru aracın seçimine, sigortalanacak varlıkların belirlenmesine, sigorta ürünlerinin genel tanıtımına, fiyatlamaya etki eden faktörlerden, doğru ürün ve teminat seçimine ve hasar süreçlerine kadar tüm sigorta konu başlıkları işletmelere rehber olması için hazırlanmıştır.

Bu bölümde ayrıca eksik sigorta kavramı incelenecek olup özellikle yapı maliyetleri, yerli ve ithal makine tesisatı ile emtia fiyatları gibi sigorta bedelinin ana kalemlerini oluşturan kıymetlerin kur dalgalanması, dünya genelindeki enflasyonist ortam gibi çeşitli sebeplerle fiyat değişikliği yaşandığı dönemde önem arz etmektedir. Eksik sigorta riskinin yönetimi ile ilgili işletmelerin alması gereken önlemler bu bölümde değerlendirilmektedir.

Türk sigorta sektörü, güçlü sermaye yapısıyla, uzman kadrolarıyla ve gelişen Dünyanın en iyi uygulamalarına öncülük etmesiyle bireylerin, işletmelerin ve nihayetinde toplumun genel direncine katkıda bulunmaya devam etmektedir.

BÖLÜM 2

İŞLETME RİSKLERİ VE YÖNETİM STRATEJİLERİ

2. İŞLETME RİSKLERİ VE YÖNETİM STRATEJİLERİ

İş dünyası, sürekli değişen ve karmaşıklaşan dinamiklere ayak uydururken bir dizi potansiyel riskle karşı karşıyadır. İşletmeler, bu riskleri etkili bir şekilde tanımlamak, değerlendirmek ve yönetmek adına kendi bünyelerinde kapsamlı bir risk yönetimi modeli oluşturmak zorundadır. Bu model, şirketlerin karşılaşabileceği çeşitli senaryolara karşı hazırlıklı olmalarını sağlamak, operasyonel sürekliliği güvence altına almak ve sürdürülebilir büyümeyi desteklemek amacını taşımaktadır.

Bu bölümde, işletmelerin kendi bünyelerinde oluşturmaları gereken risk yönetimi modelinin temel unsurlarını ele alacağız. Temel yangın risk yönetimi ve önlemlerinden başlayarak, kriz yönetimi, olay yönetimi, bilgi güvenliği riskleri, bilgi teknolojileri hizmet sürekliliği riski ve tedarikçi riskleri gibi kilit alanlara odaklanarak, işletmelerin bu riskleri nasıl yönetebileceklerini detaylı bir şekilde inceleyeceğiz.

Çalışmanın işletmelerin sadece günlük operasyonlarına değil, aynı zamanda gelecekteki belirsizlikleri de göz önünde bulundurarak sağlam bir risk yönetimi altyapısı oluşturmalarına rehberlik etmesi amaçlamaktadır. İşletme bünyesinde kurulacak etkili bir risk yönetimi modeli, işletmelerin sadece risklerini en aza indirmekle kalmaz, aynı zamanda fırsatları değerlendirme ve sürdürülebilir başarıya odaklanma konusunda da bir çerçeve sunar.

2.1. Temel Yangın Risklerinin Yönetimi

Risk veya riziko, bir işletmenin amaç ve varlığını olumsuz etkileyecek olay ve durumların gerçekleşme olasılığı olarak tanımlanır. Risk aynı zamanda belirsizlikle kasıtlı etkileşim olarak da tanımlanabilir. Belirsizlik olası, ancak tahmin edilemeyen, ölçülemeyen ve/veya kontrol edilemeyen sonuç olup; risk bu sonuca rağmen karar almanın veya riski kontrol edecek aksiyonları yeterince almamanın bir neticesidir.

Sigorta sektörü için risk analizi çalışmaları poliçede verilecek olan teminatlar açısından sigortaya konu varlıklara yönelik; tehlikelerin tanımlanması, risklerin tespit edilmesi

risklerin önlenmesi ve/veya etkilerinin azaltılabilmesi için alınabilecek tedbirlerin belirlenmesini kapsayan bir süreçtir.

Sigorta; olay/hasar sonrası destek hizmeti iken, Risk Mühendisliği; olay/hasar öncesi riski azaltma/önleme çalışmaları yapar.

Sigortaya konu tesislerde öncelikli konu mevcut risklerin iyi analiz edilerek gereken önlemlerin alınması yönünde olmalıdır. Zira bu tip işyerleri sigortalı olsalar dahi gerekli önlemler alınmaması durumunda yaşanması olası hasarlarda zararın boyutları sigorta kapsamına alınabilecek değerlerin çok daha üzerinde olabilir. Bu hasarları genellikle uzun iş kaybı süreçleri takip eder. Üretimin durması nedeniyle finansal kayıplar ortaya çıkar ve hatta parayla ölçülemeyen can kayıpları dahi yaşanabilir. Bu görüşten hareketle aşağıda belirtilen risk iyileştirici önlemlerin dikkate alınması önem arz etmektedir.

2.1.1. Genel Önlemler

Sigortaya işyerlerindeki elektrik tesisatı, kısa devre hesapları, yalıtım hesapları, bağlantı ve tespit elemanları, uzatma kabloları, elektrik tesisat projeleri ve kuvvetli akım tesisatı; 4/11/1984 tarihli ve 18565 sayılı Resmi Gazetede yayımlanan Elektrik İç Tesisleri Yönetmeliğine, 21/8/2001 tarihli ve 24500 sayılı Resmi Gazetede yayımlanan Elektrik Tesislerinde Topraklamalar Yönetmeliğine, 30/11/2000 tarihli ve 24246 sayılı Resmi Gazetede yayımlanan Elektrik Kuvvetli Akım Tesisleri Yönetmeliğine ve ilgili diğer yönetmeliklere ve standartlara uygun olarak tesis edilmelidir.

1. Özellikle üretim faaliyetinin olduğu rizikolarda, elektrik tesisatının bakımlı olması, topraklamanın yapılmış olması ve dolayısıyla statik elektrik riskinin bertaraf edilmiş olması, kablo kanalları ya da ex-proof (parlamaya karşı korumalı) tesisat kullanılmış olması gibi önlemler, kısa devre ve bunun gibi elektriksel nedenlerden kaynaklanan yangın riskini düşürecektir. Tesisatın gerek yapının fiziksel özelliklerine gerek içeride bulunan makine-tesisat ve elektronik cihazların elektriksel ihtiyaçlarına, gerekse de rizikonun bulunduğu bölgenin teknik şartlarına göre yapılması anlamında, profesyonel destek alınmış olması ve bu desteğin periyodik bakımlar ile sürdürülmesi gereklidir.

2. İşyerlerinde alınması gereken tüm yangın önlemleri Türkiye Binaların Yangından Korunma Yönetmeliği'nde belirtilen hükümlere uygun olarak tesis edilmelidir. Bu hükümlere göre,

   - Uygun tip ve sayıda portatif yangın söndürme cihazı bulundurulmalıdır. Her bağımsız bölüm için en az 1 adet olmak üzere, beher 250 m² taban alanı için 1 adet 6 kg'lık Portatif Yangın Söndürme Cihazı ilave edilerek uygun tipte söndürme tüpleri dışarıya doğru, geçiş boşluklarının yakınına ve dengeli dağıtılarak görülebilecek şekilde işaretlenerek her durumda kolayca girilebilir yerlere yerleştirilmelidir. Portatif yangın söndürme cihazlarının çevresinde emtia istifi yapılmamalı, cihazların efektif kullanım koşulları sağlanmalıdır.
   - Bu tip mahallerde, yangın su tesisatı ve dolabı sisteminin tesis edilerek, uygun kapasite ve kriterlerde su deposundan, jeneratöre direk hatla bağlı uygun kapasite pompalarla desteklenmesi gerekir. Basınçlandırma genel olarak aşağıda anlatılan tipte olmalıdır. Kullanılan pompalar yangın sistemleri için özel olarak üretilmiş, yüksek debi ve basınçta akış sağlayabilen özellikte olmalıdır. Pompalar genelde paket tip olarak kullanılır;
     i. 2 x Elektrikli Pompa sistemi
     ii. 1 Elektrik + 1 Dizel Pompa sistemi

     Yangın pompaları bakımlı olmalı, pompa odası düzenli, temiz ve gereksiz yangın yükü oluşturan malzemelerden (âtıl malzemeler, lastikler, kartonlar, kullanılmayan kablolar, ahşap paletler vb.) arındırılmış olmalıdır.

     Kimyasal ürün kullanılan bölümler için sistemin köpük destekli olması gereklidir.

   - Hidrantlar arası mesafe çok riskli bölgelerde 50 m, riskli bölgelerde 125 m, az riskli bölgelerde 150 m alınmalıdır. Bu konu dikkate alınarak, 50 m aralıklarla hidrant sistemi tesis edilmelidir. Sistem binalara 10-15 m mesafede olmalıdır.
   - Yangın dolap ve hidrantları periyodik olarak test edilerek pompaların otomatik olarak devreye girdiğinden, yeterli basınç ve miktarda su sağladığından emin olunmalıdır.

- Kaçış yolları her zaman aydınlatılmış durumda olmalıdır. Acil durum aydınlatma noktaları; bütün kaçış yolları, toplanma için kullanılan yerler, yüksek risk oluşturan makineler, elektrik dağıtım ve jeneratör odaları, pompa istasyonları, ilk yardım ve emniyet ekipmanının bulunduğu yerler, yangın uyarı butonları, yangın dolapları, yangın söndürme tüpleri ve diğer yangınla mücadele ekipmanının bulunduğu yerler olmalıdır. Bu anlamda, acil ışıklandırma sistemi kullanılabilir, ayrıca yönlendirme levhaları bulunmalıdır.

  İşyerlerine olası bir yangını erken safhalarda algılayabilmek adına uygun tipte yangın algılama sistemi kurulması (parlama riski olan bölümlerde alev veya ısı dedektörleri diğer bölgelerde duman veya ısı dedektörleri) gereklidir. Otomatik yangın algılama sistemi kurulum standartları Tablo 1'de verilmiştir.

Tablo 1:

		Yapı Yüksekliği (m)	Bina toplam kapalı alanı (m^2)
1. Konutlar		>51,50	-
2. Konaklama Amaçlı Binalar		>6,50	>1000
3. Kurum Binaları	Eğitim Tesisleri	>21,50	>5000
	Yataklı Sağlık Tesisleri	>6,50	>1000
	Ayakta tedavi ve diğer sağlık tesisleri	>21,50	>2000
4. Büro Binaları		>30,50	>5000
5.Ticaret Amaçlı Binalar (1)		> 12,50	>2000
6.Endüstriyel Amaçlı Yapılar (2)		>21,50	>7500
7.Toplanma Amaçlı Binalar	Yeme içme	>12,50	>2000
	Eğlence	>12,50	>2000
	Müze ve sergi alanları	>6,50	>5000
	Terminaller	> 6,50	>5000
8. Depolar		>6,50	>5000
9. Yüksek Tehlikeli Yerler		>6,50	>1000

(1) Sebze ve meyve halleri, balık halleri, et borsaları, metal yedek parça bulunan yerler ile benzeri yangın riski olmayan yerler hariç.
(2) Metal işleme ve montaj vb yangın riski olmayan yerler hariç.

3. İşyeri personeline özellikle manuel yangınla mücadele ekipmanlarının kullanımları konusunda hem teorik hem de pratik eğitimler verilmeli ve periyodik olarak tatbikat düzenlenmelidir. Eğitim programlarına iş kazası ve meslek hastalıkları ile ilgili konuların da eklenmesi önerilmektedir.

4. İşletmelerde "Sıcak Çalışma İzni" olması gerekir. Sıcak çalışma izni, kaynak ve kesme işlemleri sırasında sıçrayan kıvılcımların zaman içinde yangın başlatmaması için alınan önlemler paketine verilen isimdir. Bu prosedürün oluşturulması için mutlaka direkt olarak faaliyette kaynak yapılması gerekliliği yoktur, herhangi bir işletme içi tamirat dahi gerekse kullanılmak durumundadır. Sıcak Çalışma İznindeki bilgiler özetlenecek olursa:
   a. Sıcak işlem yapılacak yerlerin, 10 metre çevresindeki kolay yanıcı, parlayıcı malzemelerin üstleri kapatılır veya yerlerinden kaldırılıp uzak bir yere taşınmalıdır,
   b. Sıcak işlemler sırasında sıçrayacak kıvılcımların yangın başlatması riskine önlem olarak, yakın çevrede bir adet taşınabilir yangın söndürücü konmalıdır,
   c. Sıcak işlem yapılacak alanların yakınında kalan boru geçişi veya başka nedenle açık kalmış olan duvarlardaki boşluklar amyantlı bez, ıslak bez, yanmaz malzemelerle kalafatlanmalıdır.
   d. Sıcak işlemlerin bitmesinden sonra asgari 3 saat, mümkünse 5 saat boyunca işlemlerin yapıldığı yerlerde sıkça devriye yapılmalıdır.
   e. Sıcak çalışma izin formu ve çalışmanın tüm süreci işletmenin İş Güvenliği Uzmanı tarafından takip edilmelidir.

5. Özellikle uzun vadede ortaya çıkan meslek hastalıklarının önlenmesi adına personele yürütülen prosese uygun kişisel koruyucu ekipman (gözlük, maske, eldiven vb.) temin edilerek sürekli kullanılmaları sağlanmalıdır.

6. İşletmelerde sigara içme alanları mutlaka oluşturulmalı ve düzenli takip edilmelidir.

2.1.2. Yanıcı ve Parlayıcı Kimyasallar Kullanan İş Yerlerinde Alınması Gereken Önlemler

Yanıcı ve parlayıcı kimyasalların kullanıldığı iş yerlerinde alınması gereken önlemler, iş sağlığı ve güvenliği açısından kritik bir öneme sahiptir. Bu tür kimyasalların bulunduğu işletmelerde hem çalışanların güvenliği hem de iş yerlerinin yangın gibi acil durumlar karşısındaki direncini artırmak adına belirli protokollerin takip edilmesi hayati önem taşımaktadır. Aşağıda, yanıcı ve parlayıcı kimyasalların yoğun olarak kullanıldığı iş yerlerinde alınması gereken temel önlemler detaylı bir şekilde ele alınmıştır. Bu önlemler, elektrik tesisatından havalandırmaya kadar çeşitli alanlarda uygulanacak tedbirleri

içermektedir, böylece işletmeler hem çalışanlarını hem de maddi varlıklarını koruma noktasında etkili bir risk yönetimi sağlayabilirler.

1. Kullanılacak elektrik tesisatının parlayıcı madde buharının yoğun olarak bulunduğu bölümlerde tüm elektriksel ekipman ile birlikte ex-proof özellik diğer kısımlarda ise etanj özellik (tüm aydınlatma armatürleri, uygun standartlarda kapak takılarak ortamdan tamamıyla izole edilmelidir) gösterecek şekilde tasarlanması önerilir.

2. Parlayıcı madde buharlarının yoğun olarak bulunduğu bölümlerin hem yangın tehlikesi hem de işçi sağlığı açısından uygun standartlarda havalandırılması çok önemlidir. Solventlerin birçoğu havadan ağır olduğu için parlayıcı madde buharının zemin seviyesinde birikeceği unutulmamalıdır. Bu sebeple havalandırmanın olabildiğince zemin seviyesine yakın yerlerden yapılmasına dikkat edilmelidir. Genel olarak, püskürtme bölmesinin açık yüzünde, aşırı püskürtmenin tamamının alınabilmesi için 30 m/dk'lık bir hıza sahip mekanik vantilasyon sisteminin olması yeterlidir. Bunun yerini dolduracak hava, dışarıdan çekilir, yani işletme boyunca her noktada belirli bir hızda hava hareketi vardır. Kapı ağızları, pencereler, merdiven boşlukları, egzoz sistemi açık oldukça rüzgâr tüneli gibi eserler. Bu şartlarda çıkacak yangınların yayılma tehlikesi çok daha fazladır.

3. Gereğinden fazla püskürtme sonucu oluşan birikimler düzenli olarak temizlenmelidir.

4. İmalat ve depolama alanlarının tamamında açık alev, yanan sigara, kıvılcım çıkaran bir çalışma, aşırı ısınmış motor, ark meydana getirecek şalter, sigorta, lamba, vb. bulunmamalıdır.

5. Hammadde olarak kullanılan solvent bazlı boya ve tiner gibi parlayıcı kimyasal maddeler yangına karşı dayanıklı ayrı bir bölümde depolanmalı ve işlem yapılan

bölüme günlük kullanım miktarı kadar getirilmelidir. Bu tip kimyasalların üretim dışı zamanlarda yangına dayanıklı ve otomatik söndürme sistemi ile korunmuş kapalı kilitli alanlarda saklanmalıdır.

2.1.3. İşletmelerde Depolama Standartları

İşletmelerde depolama standartları hem çalışanların güvenliği hem de işletme sürekliliği açısından büyük bir öneme sahiptir. Depolama alanlarının düzenli, güvenli ve etkili bir şekilde kullanılması, yangın, deprem gibi acil durumlar karşısında alınacak önlemlerle doğrudan ilişkilidir. Bu bağlamda, işletmelerin depolama süreçlerini düzenlemeleri, istif alanlarını doğru bir şekilde kullanmaları ve güvenlik standartlarına uygun hareket etmeleri hem iş sağlığı hem de işletme verimliliği açısından kritik bir faktördür. Aşağıda, işletmelerde depolama standartlarına dair temel prensipler ve alınması gereken önlemler detaylı bir şekilde ele alınmıştır. Bu yönergeler, depolama alanlarının etkin bir şekilde kullanılmasını ve olası risklere karşı korunmayı amaçlamaktadır.

Depolama alanı düzgün ve düzenli olmalıdır. İstif aralarında koridorlar bırakılmalı, tavandan 50-100 cm arası mesafe bırakılarak yüksek ve yoğun olmayan depolama yapılmalıdır. Aydınlatma armatürleri altında istif yapılmamalı, aydınlatma armatürlerinin izdüşümleri yürüyüş koridorları olarak açık tutulmalıdır. Armatürler kapaklı olmalıdır.

1. İstifleme yapılan alanlarda devrilmeye karşı önleme amaçlı gerekli sabitlemeler yapılmalıdır.

2. Depolama ve üretim alanları birbirinden ayrılmalıdır. Üretim alanı içerisinde ve makineler arasında depolama veya depolama alanlarında gelişigüzel ve yüksek depolama yapılmamalıdır.

3. Dış sahada yapılan depolamanın sundurma altında olması, atıkların binadan uzak ve düzenli bir sahada stoklanması ve belirli aralıklar ile bertaraf edilmelidir.

4. Forklift şarj cihazlarının yakın çevresinde yanıcı malzeme depolaması yapılmamalıdır. Forklift kullanılmayan zamanlarda tüm kapalı alanların dışında, kendi garajlarında tutulmalıdır. Elektrikli forkliftler için akü şarj üniteleri özel havalandırılmış alanlarda olmalıdır.

2.1.4. Endüstriyel Tesislerde Çevresel Riskler

Endüstriyel tesislerin planlanması ve kurulması, çeşitli çevresel riskleri dikkate almayı gerektirir. Bu riskler, değişen iklim şartları, topografik faktörler ve çevresel etkileşimlerle birlikte ortaya çıkabilir. Bu nedenle, bir endüstriyel tesisin projelendirilmesi aşamasında, çevresel faktörlerin önemli bir rol oynadığı unutulmamalıdır. Bu bölümde, endüstriyel tesislerde çevresel risklerin nasıl ele alınması gerektiğine dair temel prensiplere odaklanılmıştır.

1. Tesislerin projelendirilmesinde değişen iklim ve topografik koşullar dikkate alınmalıdır. Güncel taşkın haritaları dikkate alınarak yer seçimleri yapılmalıdır.

2. Tesis yer seçiminde komşu firmaların da faaliyetleri dikkate alınmalı, emniyetli mesafelerde yapılar inşa edilmelidir.

3. Orman arazilerine güvenli mesafelerde yer seçimleri yapılmalıdır.

4. Kritik yardımcı işletmeler için (trafo, doğalgaz istasyonu, LPG tank sahası vb.) açık sahada yabani ot vb. temizliği düzenli olarak yapılmalıdır.

2.1.5. Bina Riskleri

Günümüzde, binaların tasarımı ve bakımı, sadece estetik ve fonksiyonalite açısından değil aynı zamanda güvenlik ve dayanıklılık açısından da kritik bir öneme sahiptir. Bu noktada, bina yapı elemanları, özellikle yangın güvenliği açısından dikkatle seçilmelidir. Aşağıdaki maddelerde dikkat edilmesi gereken kritik hususlar listelenmiştir

1. Binalarda yangın yayılımı açısından yapıda kullanılan kaplama türü önemlidir. Yanıcılık ve yangın iletme özelliği yüksek olmayan (taşyünü, camyünü gibi) malzemeler seçilmelidir.

2. Binalarda kapasite artışı yapılması, yenilenebilir enerji montajı (özellikle çatılarda) yapılması durumunda binaların statik uygunluğunun kontrolü mutlaka yapılmalıdır.

3. Binaların çatı ve oluk temizliklerinin her sene düzenli yapılmalı, çatı kaplama malzemeleri periyodik gözden geçirilmeli ve ihtiyaç doğduğu takdirde değiştirilmelidir.

2.2. Kriz Yönetimi

Kriz yönetimi, bir kuruluşun faaliyetlerini kesintiye uğratabilecek veya itibarını tehlikeye atabilecek kritik bir olayın tanımlanması ve bu olaya müdahale edilmesine yönelik süreç ve stratejilerin oluşturulmasıdır.

Krizler kuruluşun güvenliğini, itibarını, iş ve hizmet sürekliliğini, mali durumunu ve müşteri ile marka sadakatini etkileyebilecek niteliktedir. Krizlerin farklı şekillerde ve nedenlerle ortaya çıkabilecek bir doğası olması nedeniyle kuruluşların önceden buna ilişkin bir yönetim stratejisine sahip olması kritiktir.

Şirketlerin karşılaşabileceği farklı çeşitli kriz türleri mevcuttur:

- **Finansal krizler**; ekonomik durgunluklar, mali sıkıntılar ve borç sorunları şirketlerin mali durumunu ciddi şekilde etkileyebilir. Bu sebeplerle kuruluşlar, finansal yükümlülüklerini yerine getirmede veya borçlarını ödemede gecikebilmekte ve finansal bir krizle karşı karşıya kalabilmektedir. Finansal krizleri önlemek adına kuruluşlar, finansal planlama, risk yönetimi ve etkili operasyonel stratejiler geliştirebilir.
- **Teknolojik krizler**; temel altyapı arızaları, bilişim sistemlerinde yaşanan sorunlar veya üretim hatlarında meydana gelen hatalar, şirketlerin operasyonlarını etkileyebilmektedir. Teknolojik krizleri önlemek ve yönetmek için, altyapının aniden çalışmaz hale gelmesi durumuna karşı yedekleme sistemlerine yatırım yapılması önem arz etmektedir. Arıza sürelerinde şikayetlerle ilgilenmek için profesyonel müşteri hizmetlerine sahip olmak,

müşterilerin kriz algısının daha iyi yönetilmesine ve işletmenin itibarını korumasına da yardımcı olacaktır.

- **İnsan kaynaklı krizler**; çalışan grevleri, iş gücü sıkıntıları, liderlik değişiklikleri veya insan kaynakları politikalarına ilişkin skandallar, şirket çalışanları, yöneticileri, ortakları hakkında çıkabilecek asıllı veya asılsız olumsuz haberler ve medya yansımaları, şirket içi krizlere yol açabilmektedir. Bu sebeple hem yasal hakların korunması hem de kurum itibarını korumak adına çalışanların yönetimine ilişkin alınacak önlemlerin belirlenmesi önemlidir.
- **Doğal afet kaynaklı krizler;** depremler, seller, kasırgalar veya yangın gibi doğal afetler, şirketlerin tesislerini, üretim hatlarını ve tedarik zincirini olumsuz etkileyebilir. Doğal afet kaynaklı krizlerden kaynaklanan kesintileri önlemek için şirketler, bölgede aşırı hava koşullarına ve doğal afetlere dayanabilecek yapılar inşa etmeli ve operasyonları en kısa sürede çalışır hale getirmek için planlar oluşturmalıdır.

Kriz Yönetim Planı

Bir kurumun krizle başa çıkma yeteneği, sadece kriz sırasında olağan iş süreçlerinin sürdürülebilmesini değil, aynı zamanda paydaşlara ve çalışanlara karşı sorumlulukların yerine getirilebilmesini de içerir. Kriz yönetimi, bu tür zorlayıcı durumlarla etkili bir şekilde başa çıkabilmek için önceden planlama, stratejik yönetim ve hızlı tepki gerektiren karmaşık bir süreçtir.

Bir kriz durumuna etkili bir yanıt verebilmek adına, kriz yönetiminden sorumlu bir ekip ve Kriz Yönetimi Komitesi'nin kurulması kritik bir öneme sahiptir. Bu ekip, krizle başa çıkma stratejilerini belirleme, kriz sürecini yönetme, paydaşlarla etkili iletişim kurma ve organizasyonun normale dönmesini sağlama gibi görevleri üstlenir. Üst yönetim temsilcileri ile iş birimi temsilcilerinin yanı sıra, iletişim, hukuk, güvenlik ve iş güvenliği ile teknoloji ve bilgi güvenliği konularında uzman personelden oluşan bir ekip, kriz yönetim sürecini etkin bir şekilde yürütebilir. Krizlerin tahmin edilemez yapısı göz önüne alınarak görevli kriz ekibi üyelerinin en az birer yedeklerinin de önceden belirlenmesi yerinde olacaktır.

Bu bölümde, kriz yönetimi planlamasının temel adımları ve bir kriz durumunda etkili bir yanıt verebilmek için alınması gereken önlemler detaylı bir şekilde ele alınacaktır. Kriz durumlarında acil eylem planlarının oluşturulması, iletişim stratejilerinin belirlenmesi, güvenli tahliye ve toplanma alanlarının planlanması gibi konular bu raporun odak noktaları arasında yer alacaktır. Ayrıca, kriz sırasında organizasyonun iş sürekliliğini sağlamak adına yapılması gerekenler ve kriz yönetimi sürecinin sürekli olarak iyileştirilmesi için alınacak önlemler on iki maddede ele alınacaktır.

1. Kriz durumuna hızlı bir şekilde cevap verebilmek adına kriz yönetiminden sorumlu bir ekip ve Kriz Yönetimi Komitesi kurulması önem arz etmektedir. Kriz yönetiminden sorumlu ekip:
    - Krizle başa çıkma stratejilerini belirlemelidir,
    - Aldıkları kararları uygulamaya koyabilecek yetkiye sahip olmalıdır,
    - Kriz sürecini baştan sona yönetmelidir,
    - Paydaşlarla etkili iletişim kurmalı ve organizasyonun hızlı bir şekilde normale dönmesini sağlamaya yardımcı olmalıdır.
    - Her üye, kendi uzmanlık alanına odaklanarak kriz durumlarına etkili bir şekilde müdahale etmeye çalışmalıdır.
    - Kriz anında etkin bir yönetim sağlamak amacıyla kriz yönetim ekibi çok kalabalık olmamalıdır.
    - Kriz senaryolarına göre önceden belirlenmiş kriz yönetim üyeleri arasından yaşanan krizin yönetiminde aktif rol alacak temsilci ve uzmanlar kriz yönetim ekibine katılması, diğer üyelerin ise hazırda beklemesi kriz yönetim ekibi katılımcı sayısını sınırlı tutmak için tercih edilebilir bir yöntem olacaktır.
    - Kriz Ekibi aşağıdaki görevleri üstlenen üyelerden oluşabilir:
        i. **Üst Yönetim Temsilcileri**: Genel müdür ve üst düzey yöneticilerden oluşur. Kriz durumlarında stratejik kararlar alır ve krizle ilgili genel yönetimi sağlar. Kriz yönetim sürecinde kriz ekibince tam anlaşma sağlanamayan konularda son kararı vermek adına bir kriz masası lideri de tanımlanmalıdır. Genellikle bu görev Genel Müdür'e verilir.

ii. **İş Birimi Temsilcileri:** Yaşanan her kriz senaryosu organizasyonun farklı iş birimlerini etkileyebileceği için, her iş birimini temsil eden yöneticilerden oluşabilir. Bu temsilciler, krizle ilgili spesifik uzmanlık alanlarından seçilmelidir.

iii. **İletişim Uzmanları**: Medya ilişkileri, iç iletişim ve halkla ilişkiler konularında uzman personelden oluşur. Kriz sırasında iletişim stratejilerini belirlemek konusunda kriz ekibini yönlendirmeli ve iletişim konusunda alınan kararları uygulamalıdır.

iv. **Hukuk Uzmanları:** Hukukçulardan ve kurumun yapısına göre hukuki konularda uzmanlaşmış sektör profesyonellerinden oluşur. Kriz durumlarında kuruluşların hukuki sorumluluklarını değerlendirmeli ve hukuki stratejiler geliştirmelidir.

v. **Güvenlik ve İş Güvenliği Uzmanları:** Çalışanların ve şirket varlıklarının güvenliğinden sorumlu uzmanlardan oluşur. Kriz durumlarında güvenlik önlemlerini planlamalı ve uygulanmasını sağlamalıdır.

vi. **Teknoloji ve Bilgi Teknolojileri Uzmanları:** Bilgi teknolojisi sistemlerini yöneten uzmanlardan oluşur. Bilgi güvenliği, veri kurtarma ve sistemlerin iş sürekliliği konularında görev almalıdır.

vii. **Kriz Müdahale Ekipleri:** Acil durum müdahale ekipleri, özellikle fiziksel kriz durumlarında (örneğin, yangın, kaza) hızlı müdahale için görevlendirilirler.

viii. **Kriz Yönetim Koordinatörü:** Kriz yönetiminden sorumlu ekibin yöneticisidir. Kriz durumunda Kriz Yönetim Lideri ile birlikte süreci koordine eder, iletişimi sağlar ve stratejik kararlar alır.

ix. **Kriz Yönetim Lideri:** Son karar belirleyici durumundadır. Kriz koordinatörü ile birlikte kriz yönetim ekibinin toplanması kararını alır. Komite üyelerinin, kriz masasında toplanmasını sağlar. Kriz masasında konuların ele alınışı ve kararların kayıt altına alınarak ilgili iş birimlerine iletilmesi gibi koordinasyon görevleri vardır.

2. Kriz yönetimi konusunu üstlenmesi ve yönetmesi adına her ekipten bir asıl bir de yedek temsilci seçilerek, görev ve sorumluluklarına ilişkin bu temsilcilere eğitimler verilmeli ve belirli periyotlarda kendilerinin de katılımı ile tatbikat ve testler gerçekleştirilmelidir.

3. Kriz durumları için Acil Eylem Planı oluşturulmalı ve planlar oluşturulurken aşağıdaki hususlar dikkate alınmalıdır:
   - Risk değerlendirmesi yapılmalı, olası acil durumlar (yangın, deprem, sel, salgın hastalık vb.) ve etkileri değerlendirilmeli, acil durumlar için bir ekip belirlenmeli ve bu ekibin görev ve sorumlulukları dokümante edilmelidir.
   - İç ve dış iletişim planları oluşturulmalı ve acil durum sırasında iletişimin nasıl kurulacağı belirlenmelidir.
   - Güvenli tahliye ve toplanma alanları oluşturularak binadan güvenli çıkış için tahliye planı oluşturulmalıdır.
   - Acil durum ekipmanları (ilk yardım ekipmanları ve acil durum malzemeleri) belirlenmeli, yangın söndürme ekipmanları kontrol edilmeli ve düzenli olarak bakımları yapılmalıdır.
   - Çalışanlara acil durum prosedürlerine ilişkin bilgi verilmeli ve düzenli periyotlarda acil durum tatbikatları düzenlenmelidir.
   - Veri yedekleme ve kurtarma planı oluşturulmalı ve iş sürekliliği yönetimi planı düzenli olarak gözden geçirilmelidir.
   - Acil durumlar için yetki ve sorumluluklar netleştirilmelidir.
   - Planlar düzenli olarak gözden geçirilmeli ve güncellenmelidir.

4. Kriz sırasında, kuruluşun yürüttüğü operasyonlarda yaşanacak aksamaları en aza indirmek ve iş sürekliliğini sağlamak büyük önem arz etmektedir. Bu sebeple, alternatif çalışma düzenlemeleri, yedekleme sistemleri ve kaynakların kritik işlevlere yeniden tahsis edilmesine yönelik süreç ve uygulamalar periyodik olarak test edilmelidir. Kritik uygulamaların ve servislerin sorunsuz bir şekilde çalışmasının sağlanması amacıyla kritik personel belirlenmeli ve belirli periyotlarda olağanüstü durum testleri ile uygulamalara erişim test edilmelidir.

5. Felaket durumunda irtibata geçilecek öncelikli çalışanların ve kuruluşların listesi yapılmalıdır. İletişim bilgileri, herkesin görebileceği ve kolayca erişebileceği bir yerde bulunmalıdır.

6. Bir kriz durumu geliştiği anda sahada uyarılacak kişi/kişiler netleştirilmelidir. Kriz yöneticisinin yanı sıra, çalışanlar arasında yaklaşan bir felaket hakkında ilk elden bilgi sahibi olan bir koordinatör gereklidir.

7. Çalışanların toplanabileceği merkezi bir lokasyon ve acil durum tahliye rotaları belirlenmelidir. Açılması kolay olan acil kaçış kapıları belirlenmeli, tanıtılmalı ve herkesin görüp anlayabileceği şekilde etiketlenmelidir. Aynı şekilde bir acil durum merkezi toplanma alanı da olmalıdır.

8. Kriz Yönetimi Prosedürü oluşturularak tüm çalışanların erişebileceği bir platformda dokümante edilmelidir.

9. Acil durum ekipmanlarının düzenli olarak veya gerektiğinde test edilmeli ve iyileştirilmelidir.

10. Kriz durumlarıyla başa çıkma konusunda düzenli eğitim ve tazeleme seminerleri düzenlenmelidir. Paydaşları acil durumlara müdahale konusunda güncel tutmak için düzenli olarak tatbikatlar ve alıştırma operasyonları yapılmalıdır. Her yıl düzenli olarak personel, çalışma lokasyonu ve sistem kaybı senaryolarının testleri yapılmalı ve sonucunda ortaya çıkan aksiyonlar giderilmelidir.

11. Kuruluşların paydaşları bilgilendirmesi, oluşan endişeleri gidermesi ve krize müdahalenin ilerleyişi hakkında bilgi sağlaması adına açık ve şeffaf iletişim kanalları kurulmalıdır. Bu, farklı kitlelere etkili bir şekilde ulaşmak için geleneksel medya, sosyal medya ve kurum içi iletişim kanalları gibi çeşitli iletişim platformlarının kullanılmasını içerebilir.

12. Krizin çözümlenmesinden sonra, krize müdahale sürecindeki eksiklikler ve gelişim alanları tespit edilerek belirlenecek süre içerisinde gelişim sağlayacak stratejiler geliştirilmelidir. Bu, kuruluşların geçmiş olaylardan ders çıkarmalarına, gelecekteki olaylara karşı kurumsal ve operasyonel dayanıklılıkları ile hazırlıklarını geliştirmelerine yardımcı olacaktır.

2.3. Olay Yönetimi

Olay yönetimi, bir kuruluşta yaşanan olayları tanımlama, önceliklendirme, bu olayları yanıtlama ve çözme sürecini ifade eder. Bu bağlamda yapılan olay tanımlaması, kuruluşu etkileyebilecek plansız olayları ifade etmektedir. Olay yönetiminin temel hedefleri:

- Yaşanan olayların etkisini en aza indirmek,
- Normal işleyişi mümkün olan en kısa sürede geri sağlamak,
- Gelecekte kuruluşun karşı karşıya kalabileceği potansiyel olayları önlemektir.

Olay yönetimi, protokollere bağlılık ve hızlı çözümün önemli olduğu her kuruluşun işleyişinde oldukça önemli bir rol oynamaktadır. Teknik arızalar, güvenlik ihlalleri ya da hizmet aksaklıkları gibi olaylar, operasyonları etkilemekte olup; kuruluşların itibarına ciddi zarar verebilmektedir. Bilgi Teknolojileri servis kesintileri, bilgi güvenliği ihlalleri, tesis güvenliği sorunları ve doğal afet etkileri ana olay yönetimi aksaklıklarına örnektir.

Olay yönetimi konusunda kuruluşların bir aksiyon planına sahip olması, olayın çözüme ulaşması konusunda oldukça önemlidir. Aşağıdaki aksiyon planları, kurum içi olay yönetimi işleyiş planını içermektedir. Yaşanabilecek olaylara karşı kurulması gereken işleyiş yapısı aşağıdaki 7 maddeyi içermelidir:

1. **Kapsamlı Bir Olay Yanıt Planı Oluşturma:**

   İyi tanımlanmış bir Olay Yanıt Planına sahip olmak olay yönetiminin en temel taşıdır. İyi hazırlanmış bir plan, herhangi bir olay yaşanması durumunda, olaya yanıt sürecine katılan takım üyelerinin rollerini ve sorumluluklarını içermelidir. Net bir eskalasyon hiyerarşisi, iletişim protokolleri ve çeşitli olay senaryoları için önceden belirlenmiş eylemleri içermelidir. Bu tür bilgileri içeren kurum

politikasının oluşturulması büyük önem arz etmektedir. Olay yanıt planı statik bir belge değil, aynı zamanda ortaya çıkan ya da ortaya çıkabilecek tehditlere ve organizasyonel değişikliklere hızlıca adapte olacak şekilde yılda bir kere gözden geçirilen ve güncellenen dinamik bir doküman olmalıdır.

2. **Olayları Sınıflandırma ve Önceliklendirme:**

Yaşanan aksaklıklar farklı önem seviyelerine sahip olabilmektedir. Olay yönetimi sürecinde, gerçekleşen olayları şiddet ve iş operasyonları üzerindeki etkilerine göre sınıflandırabilmek önemlidir. Bu amaçla olayları önceliklendirmek için bir sınıflandırma sistemi oluşturulmalıdır. Olaydan etkilenen hizmetlerin kritikliği, olayın kapsamı (genel kesinti, kısmi kesinti, fonksiyonel hata vb.), tahmin edilen olay süresi gibi kıstaslar bu sistemin oluşturulmasında kullanılabilir. Oluşturulan bu sisteme göre olaylara yanıt verecek olan ekip öncelikli sorunlara odaklanabilmelidir. Bu da önemli ve etkisi yüksek olacak olaylara erken müdahale etme fırsatı verecektir. Sınıflandırma kriterlerinin düzenli olarak gözden geçirilmesi, değişen iş öncelikleri ve risk ortamına uygunluğu sağlayacaktır. Süreçleri sürekli olarak gözden geçirme, olaylara müdahale etmek kadar önem arz etmektedir.

3. **Hızlı ve Doğru Olay Tanımlama:**

Olayları erken tespit edebilme, olay yönetiminin temel yapı taşlarından biridir. Sıradan işlemlerden sapmaları veya olağan dışı aktiviteleri hızlı bir şekilde tanımlayabilen izleme araçlarına ve sistemlere sahip olmak oldukça önemlidir. Bu proaktif yaklaşım, potansiyel olayı önleyerek henüz gerçekleşmeden müdahale etme imkânı sağlayacaktır. İzleme yeteneklerinin güncellenmesi ve teknolojik gelişmelerin takip edilmesi bu sürecin gelişmesine katkıda bulunacaktır.

4. **Net İletişim Protokolleri:**

Etkili iletişim, olay yönetiminin önemli bir parçasıdır. Olay Müdahale Ekibi, süreç ile ilişkili departmanlar arasında ve gerektiğinde dış paydaşlarla bilgi paylaşımını belirleyen net ve bilgilendirici iletişim protokolleri geliştirmelidir. İletişim protokolleri, süreç içinde yer alması gereken herkesin bilgilendirilmesini ve yanlış

bilgi aktarım riskinin en aza indirilmesini sağlar. Yüksek stresli olaylar sırasında bilgiyi hızlı ve doğru bir şekilde iletmek önemlidir. Ayrıca iletişim tatbikatları düzenleyerek kurumlar gerekli gözden geçirmeleri sağlamalıdır.

5. **Olay Takip Sistemi Uygulanması:**

   Olay takip sistemi uygulaması, tüm olay yönetimi sürecinin dokümante edilmesine yardımcı olacaktır. Bu sayede başından sonuna kadar tüm süreç kayıt altına alınacak ve böylece iyileştirme adımları ile süreç içindeki öğrenimler de dokümante edilecektir. Benzer olayların ileride tekrarlaması durumunda ilk olayda uygulanan çözüm adımlarına hızlıca ulaşılabilecektir. Olay takip sistemi kayıtları sayesinde olay yönetimi sürecine şeffaflık ve denetlenebilirlik ölçütleri sağlanmaktadır. Ayrıca sürekli iyileştirme için olay sonrası yapılacak analizlerde sürecin takibi sağlanabilmektedir.

6. **Düzenli Eğitim ve Tatbikatlar:**

   Olay yönetimi konusunda iyi hazırlanmış eğitimlere ve iyi eğitilmiş ekiplere sahip olmak sürecin doğru yönetilmesine katkı sağlar. Müdahale Ekibinin tecrübeli olması ve rollerini etkin bir şekilde gerçekleştirebilmeleri adına eğitimler verilmelidir. Bu eğitimler hem kuruluşta hem de farklı sektörlerde yaşanmış olayları içermelidir. Verilen eğitimler, kurumun vizyon ve misyonuyla örtüşmelidir. Ayrıca simülasyon çalışmalarının düzenlenmesi de oldukça kritiktir. Bu eğitimlerde devamlılığı sağlamak kadar eğitime katılan kişilerin başarılarını ölçümlemek de sürecin benimsendiğini anlamak adına önemlidir.

7. **Olay Sonrası Analiz ve Raporlama:**

   Olay çözümlendikten sonra kök nedenlerin belirlenmesi kritiktir. Kök nedenlere göre detaylı gelişim alanı/alanları belirlemek olay sonrası analizin bir zorunluluğudur. Bu noktada belirlenen planların takibinin yapılması da gerekmektedir. Yaşanan olay sonrasında çıkarılan dersler belgelenmeli ve olay yanıt planı çıkarılan derslere göre şekillendirilmelidir. Ayrıca olaya dahil olan ekiplere geri bildirim döngüsü de oluşturulmalıdır. Bu tür olayları organizasyon geneline yayarak kuruluş içinde bilinç oluşturulması fayda sağlayacaktır.

2.4. Bilgi Güvenliği Riskleri ve Yönetimi

Bilgi güvenliği; hassas, kişisel, ticari sır ya da bir kuruluş için kritik olarak kabul edilen her bilgi unsurunu; yetkisiz erişimler, kayıplar veya sızıntılara karşı koruma prosedürlerini tarif etmektedir. Kuruluşlara ait bu bilgilerin yazılı, sözlü ya da dijital kanallarda korunması gerekmektedir. Hassas ya da gizli bilgilerin organizasyon dışında kullanımının ya da sızmasının engellenmesi için alınması gereken tüm önlemler, bilgi güvenliği prosedürleri kapsamında değerlendirilmektedir.

Bilgi güvenliği uygulamaları, bir kuruluş için temelde bilginin, üç boyutta ele alınması (CIA Prensibi) üzerinde kurgulanmıştır: Gizlilik (Confidentiallity), Bütünlük (Integrity) ve Erişilebilirlik (Availability).

- Gizlilik, hassas ya da gizli verilerin yalnızca yetkili kişiler ya da sistemler tarafından görüntülenerek verilerin yetkisiz kişilere sunulmaması anlamına gelmektedir. Saldırılara karşı şifreleme standartlarının oluşturulması, kimlik ve erişim yönetim süreçlerinin olgunlaştırılması, görevler ayrılığı ve yetkilendirmelerin riskleri azaltacak şekilde oluşturulması ve VPN (Virtual Private Network) gibi uygulamalar bilgi gizliliğinin korunmasına yönelik önlemlere örnek olarak gösterilebilir.
- Bütünlük, bilgi sistemleri içerisinde veya fiziksel olarak tutulan bilgilerin değiştirilmediğinden ya da bilgi kaybının olmadığından emin olunmasıdır.
- Erişilebilirlik, sistem ya da fiziksel bilgilerin, organizasyon içerisinde kolay kullanılabilirliğinin sağlanmasıdır.

Bilgi güvenliği uygulamaları, yukarıda bahsi geçen üç unsur etrafında şekillenmekte olup; yerel ve uluslararası birçok perspektif belirlenmiştir. Temelde;

- ISACA (Information Systems Audit and Control Association) tarafından oluşturulan COBIT (Control Objectives for Information and Related Technology) standartları,

- Bankalar için Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) tarafından oluşturulan "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik", ve
- ISO/IEC 27001 Bilgi Güvenliği Yönetim Sistemi Standardı
- NIST CSF

bilgi güvenliği uygulamaları için işletmelere, bir çerçeve oluşturabilmek için rehberlik eden standartlara örnek olarak verilebilir.

Bilgi güvenliği süreçlerinin etkin kurgulanmadığı kuruluşlarda yaşanan bilgi güvenliği olayları; operasyonel kayıplara, cezai yaptırımlara, itibar kayıplarına ve finansal kayıplara (gelir ve fırsat kaybı) neden olabilmektedir. Ayrıca kuruluş içerisinde nitelikli ve fikri mülkiyet kapsamında değerlendirilen verilerin ve kişisel verilerin çalınmasına, rakip organizasyonların bu verileri kullanarak pazarda üstünlük sağlamasına neden olma riski bulunmaktadır. Bu risklere ek olarak, iş süreçleri için gerekli verilerin kaybı, iş sürekliliğini olumsuz etkileyecektir.

Bilgi güvenliği uygulamalarının temelinde kuruluşun, sahip olduğu bilgileri iyi tanıması ve tanımlaması gerekmektedir. Kuruluş, sahip olduğu bilgilere hâkim olduğu düzeyde bilgilerini koruyacak kontrolleri tasarlayabilecektir. Bilgi güvenliği prosedürlerinin etkinliği de sahip olunan bilginin tanınmasıyla doğru orantılıdır. Kuruluş içerisindeki tüm bilgiler öncelikle belirlenmeli, sonrasında değerlendirilmeli ve sınıflandırılmalıdır. Sınıflandırma yapılırken her bir bilgi için risk analizi gerçekleştirilmeli ve risk analizi sonucuna göre kritiklik derecesi belirlenmelidir. Kritiklik derecesi gizli, hassas, sır kapsamında ya da kişisel veri gibi, kurumun ihtiyaçları ile paralel olarak tanımlanmalıdır. Bu kapsamda bir veri envanterinin oluşturulması, bilgilerin takibinin kolaylaştırılmasını ve bilginin kataloglanarak kontrol edilmesine kolaylık sağlayacaktır. Veri envanterinin yanı sıra, takip edilen ya da edilmesi hukuken gerekli olan standart ve mevzuatın gerektirdiği diğer envanterlerin de (varlık envanteri, kişisel veri işleme envanteri gibi) oluşturulması gerekmektedir.

Veri mimarisinin oluşturulması ve tüm verilerin oluşturulan mimariye uygun şekilde sistemlerde işlenmesinin sağlanması, bilgi güvenliği süreçlerinin etkin işletilmesinde kritik bir role sahiptir. Bahsi geçen aşamalardaki eksiklikler, kuruluşların bilgi güvenliği prosedürlerini uygulamalarında körlük oluşturarak, kuruluştaki tüm verilerin korunmasını sağlamakta başarısız olunması riskini ortaya çıkaracaktır.

Sahip olduğu bilgileri iyi tanıyan ve tüm verilerine büyük ölçüde hâkim olan, risk yönetimi stratejilerini, iş stratejileri ile uyumlu duruma getirmiş bir kuruluş, bilgi güvenliği uygulamalarında alacağı önlemleri sahip olduğu verilere uyguladığı sınıflandırma yapısına göre oluşturmalıdır. Kuruluşların bu aşamada kendi bilgi güvenliği süreçlerini oluşturacak kapsayıcı bir politika oluşturması büyük önem arz etmektedir. Bilgi Güvenliği Politikası içerisinde tüm bilgi unsurlarını tanımlamalı ve ilgili unsurlara ilişkin alacağı güvenlik önlemlerini belirlemelidir.

Kuruluş, CIA Prensibine uygun olacak şekilde **"gizlilik" kapsamında;**

- Bilgi güvenliği farkındalığını artırma amaçlı eğitimler ve çalışmalar gerçekleştirmeli,
- Kimlik ve erişim süreçlerini kurgulamalı,
- Minimum yetkilendirme, sıfır güven ve görevler ayrılığı gibi bilgi güvenliği ilkelerini gözetecek şekilde erişimleri yönetme amacıyla bir yetkilendirme mekanizması oluşturmalı,
- Güncel ve onaylı kriptografik yöntemler kullanarak verileri ve veri kanallarını şifrelemeli,
- Ağ güvenliği için internete açık ve kapalı olacak şekilde kritik ile kritik olmayan sunucularını belirlemeli ve ayrıştırmalı,
- Güvenlik duvarı çözümlerini kullanmalı, konfigüre etmeli ve yalnızca belirli kullanıcıların ağa erişimini sağlamalı,
- Endpoint Detection and Response (EDR) çözümleri kullanarak son kullanıcı veri çıkış noktalarını kontrol altına almalı,
- Veri maskeleme yöntemlerini gerektiği ölçüde kullanmalı,
- Uzaktan bağlantıları kontrol etmek için VPN kullanmalı,
- Dış bağlantıları takip edecek teknolojik çözümler kullanmalı,

- Network-Based Intrusion Prevention (NIPS) yöntemleri kullanarak zararlı yazılımlardan korunmalı ve olası sızmaların tespiti ile engellenmesi için güvenlik önlemleri oluşturmalıdır.

"Bütünlük" kapsamında;

- Sistem ve veri tabanlarında yetkisiz erişimleri engelleyecek kontrolleri oluşturmalı,
- Veri tabanlarına yetkisiz erişimleri ve veri tabanında gerçekleştirilen "DML" ve "DDL" komutlarını kaydetmeli/kayıt altına almalı, kayıtlardan (loglardan) alarmlar elde edecek ve aksiyon alacak şekilde takip mekanizması kurgulamalı,
- Sistemlerini yedeklemeli,
- Veri merkezleri için fiziksel güvenlik önlemlerinin alındığından emin olmalı,
- Felaket kurtarma merkezi (DRC) oluşturarak verilerinin ilgili merkezde yedeklendiğinden emin olmalı,
- Yedekten geri dönüş için süreç tasarımları yapmalı ve geri dönüş kabiliyetlerini düzenli olarak kontrol etmeli,
- Cihaz bakımlarının, versiyon güncellemelerinin ve yama uygulamalarının takip edilmesini sağlayacak yama ve konfigürasyon yönetimi süreçleri tasarlanmalı, uygulanmalıdır.

"Erişilebilirlik" kapsamında;

- Veriyi kullanıma kolay hale getirecek raporlama araçları ve uygulama ara yüzleri tasarlamalı,
- Hızlı veri transferi gerçekleştirecek teknolojik altyapıları kullanmalı,
- Sistemlerini ve cihazlarını yük ve performans testleri ile kontrol etmeli, düzenli olarak takip edecek otomatize süreçler işletmeli,
- Kapasite planlamalarını, kullanıcılarına kesintisiz hizmet verecek şekilde gerçekleştirmeli,
- İş ve servis sürekliliği için İş Sürekliliği Yönetimi ve Bilgi Teknolojileri Servis Sürekliliği Fonksiyonlarını oluşturmalı,

- Uygulamalar ve servisler için iş etki analizleri gerçekleştirmeli ve analizler sonucunda kesintiler ile başa çıkmak için iş sürekliliği planları oluşturmalı,
- Kullanıcılarına hızlı şekilde destek sağlayabileceği, etkin yardım masası süreçlerini tasarlamalı,
- Problem ve olay yönetimi için bir fonksiyon oluşturmalı, problem ve olayların hızlı çözüme kavuşacağı şekilde işletmeli,
- Kullanıcılarına, işin yapılması için teknolojik açıdan yeterli imkanları sunmalıdır.

Kuruluşlar, bilgi güvenliği uygulamalarını devreye aldıklarında, bahse konu "CIA Triad" modeline uygun şekilde bilgilerini güvenceye alabilecek ve bilgiler üzerindeki riskleri, bilgi güvenliği prosedürlerinin etkinliği ölçüsünde ortadan kaldırabilecek ya da azaltabilecektir. Ancak, riskleri bilgi sistemleri içerisinde tamamen ortadan kaldırmak çoğunlukla mümkün olmamaktadır. Kötü niyetli aktörler ya da içeriden kaynaklı sızıntıları önlemek zor olacaktır. Bu noktada ise bilgi güvenliği farkındalığını artıracak önlemler ve bilgi güvenliği olaylarına karşı yaptırımlar önem kazanmaktadır. İçeriden ya da dışarıdan herhangi bir sızıntı ya da saldırı ihtimali her sistem için mevcut bir risktir. Siber güvenlik saldırılarının yaşanması ya da içeriden bilgi sızdırılması durumlarında, yani bir bilgi güvenliği olayı gerçekleştirildiğinde, olayın tespiti ve çözümü için bilgi güvenliği olay yönetimi süreçlerinin etkinliği önem kazanmaktadır. Bilgi güvenliği olayının tespiti, sorgulanması ve alınacak aksiyonların belirlenmesi süreç yönetiminde iyi kurgulanması ve etkin işletilmesi gereken adımlardır. Cezai yaptırımlara sebep olabilecek her türlü olay için yeterli kanıt toplanmalı ve güvenli şekilde saklanmalıdır. Sızma testleri ile sistemler sürekli test edilmeli ve siber saldırılardan kaynaklanacak olaylar, tatbikatlarla test edilmeli ve uygun yöntemler ile çözüm sağlanmalıdır.

2.5. Bilgi Teknolojileri Hizmet Süreklilik Riski ve Yönetimi

Bilgi Teknolojileri Hizmet Sürekliliği Yönetimi, bilgi ve iletişim teknolojisi hizmetinin ani bir felaket nedeniyle zarar görmesi veya devre dışı kalması durumunda kurtarma için acil durum planlamasını, servislerin ve uygulamaların kesintiye uğramasının önüne geçilmesi için alınan önlemleri ve aksiyonları içeren bir süreçtir. BT Hizmet Sürekliliği

Yönetimi'nin temel amacı, iş sürekliliği için gerekli servislerin sürekliliğini sağlamak ve iş sürekliliği süreçlerini desteklemektir. Bu yönetim tipi temelde felaket durumları ele alınarak tasarlanmakta olup; olası felaket senaryolarında, bilgi teknolojilerinin operasyonlarının kesintiye uğramasının önüne geçilmesine odaklanmaktadır. Küçük teknik sorunlar ve problemler, Problem ve Olay Yönetimi kapsamında değerlendirilmekte olup bu konu başlığı altında ele alınmamaktadır.

BT Hizmet Sürekliliği Yönetimi için rehber olarak;

- ITIL (Information Technology Infrastructure Library),
- ISACA (Information Systems Audit and Control Association) tarafından oluşturulmuş COBIT uygulamaları,
- Yerel olarak hazırlanmış "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik"
- ISO 22301 İş Sürekliliği Yönetim Sistemi Standardı

göz önünde bulundurularak süreçler dizayn edilebilir.

BT Hizmet Sürekliliği Yönetim sürecinin eksikliği ya da hatalı tasarlanması durumunda kuruluşlar, servis kesintileri ile karşı karşıya kalabilecek olup; bu durum iş süreçlerinin aksamasına neden olacaktır. Sistem arızaları ve iş kesintilerine ilişkin kuruluşların kurtarma planlarının olmaması ya da bu planların etkin bir şekilde oluşturulmadığı durumlarda, herhangi bir sorun anında öncelikle bilgi sistemlerinin, devamında ise iş sürekliliğinin sürdürülebilirliği tehlikeye girecektir. Sonucunda ise kuruluş; finansal kayıplar(gelir ve fırsat kaybı),operasyonel kayıplar ve itibar kaybı ile karşı karşıya kalacaktır. Bu nedenle, kuruluşların etkin bir BT Hizmet Sürekliliği Yönetim süreci tasarlaması ve işletmesi kritik önem taşımaktadır.

İş Sürekliliği Yönetimi, mevcut iş süreçlerinin felaket anlarında dahil devamlılığını sağlayacak uygulamalar ve önlemler olarak değerlendirilmektedir. Her kuruluş, özellikle kritik iş süreçlerinin devamlılığını tehdit edecek riskleri belirlemeli ve BT Risk Yönetimi kapsamında ele almalıdır. İş süreçleri için felaket durumunda alınacak fiziksel güvenlik önlemlerine ek olarak, iş etki analizleri gerçekleştirilmelidir. İş sürekliliği planları ve iş etki

analizleri, belirlenen riskler doğrultusunda oluşturulmaktadır. BT Hizmet Sürekliliği Yönetimi süreçleri, bu aşamaya paralel olarak BT tarafındaki hizmet kesintilerini önceden belirleyebilmek için risk ve etki analizleri gerçekleştirilerek işletilmektedir. Etkin bir süreç tasarımı için öncelikle BT hizmetleri ve BT varlıkları net bir şekilde belirlenmelidir. Belirlenen hizmetlerin ve varlıkların envanterinin oluşturulması ve bu envanter içerisinde risk düzeyine göre sınıflandırılması takip edilebilirlik açısından avantaj sağlamaktadır. İş sürekliliği ve BT hizmet sürekliliği için prosedürler oluşturulmalıdır. İş stratejileri ile uyumlu, BT Hizmet Sürekliliği ve İş Sürekliliği stratejilerinin belirlenmesi, kesintiye sebep olacak olay ya da felaket durumlarındaki kurtarma stratejilerinin daha net şekilde belirlenmesini sağlamaktadır.

Süreç hedefleri temel olarak dört başlık altında tanımlanabilmektedir:

1. BT Hizmet Sürekliliği Yönetimi destek süreci hedefi; felaketlerle mücadelede sorumlulukları olan tüm BT personeli üyelerinin görevlerini tam olarak bildiklerinden emin olmak ve bir felaket meydana geldiğinde ilgili tüm bilgilerin hazır olduğundan emin olmaktır.

2. Hizmetlerin sürekliliği için tasarım hedefi; iş etki analizleri sonucunda kararlaştırılan iş sürekliliği hedeflerini karşılamak için uygun ve maliyet açısından karşılanabilir süreklilik mekanizmaları ve prosedürlerinin tasarlanması olarak tanımlanabilir. Bu hedef, risk azaltma önlemlerinin ve kurtarma planlarının tasarımını içermektedir.

3. BT Hizmet Sürekliliği Yönetimi eğitim ve testleri hedefi; afet durumları için tüm önleyici tedbirlerin ve kurtarma mekanizmalarının düzenli olarak test edildiğinden emin olmak amacıyla gerçekleştirilen faaliyetleri içermektedir.

4. BT Hizmet Sürekliliği Yönetimi gözden geçirme hedefi; felaket önleme tedbirlerinin, iş tarafındaki risk algılarıyla uyumlu olup olmadığını gözden geçirmek ve süreklilik tedbirlerinin ve prosedürlerinin düzenli olarak sürdürüldüğünü ve test edildiğini doğrulamaktır.

BT Hizmet Sürekliliği Yönetimi kapsamında işletmeler;

- Acil durum senaryoları oluşturmalı,
- Acil durum senaryolarında alınacak aksiyonları belirlemeli ve tatbikatlar yapmalı,
- İş sürekliliği planlarını, hizmet sürekliliği süreçlerini kapsayacak şekilde tasarlamalı,
- Uymaktan sorumlu olduğu regülasyon, yönetmelik vb. mevzuatın iş sürekliliği konusundaki gerekliliklerini göz önünde bulundurmalı,
- İş etki analizlerini her servis için gerçekleştirmeli, iş birimleri tarafından kullanılan uygulamalara ek olarak BT ekipleri tarafından kullanılan servisler arası bileşenler, servis monitör sistemleri, ağ bileşenleri, otomasyon sistemleri, bilgi güvenliği sistemleri vb. bileşenler de iş etki analizi çalışmaları kapsamına dâhil edilmeli,
- İş etki analizlerinin, her servisin ilgili servis sahibi iş birimi veya BT birimi tarafından gerçekleştirildiğine emin olunmalı, özellikle iş birimi sahipliğindeki uygulamalar için iş etki analizi çalışmalarının BT birimlerince yapılması gerekmesinin önüne geçmeli, iş birimleri de bu teknik değerlemelere katılmaya teşvik edilmeli,
- Bulut sistem sağlayıcıları ve kritik tedarikçileri belirleyerek servis devamlılığı için kendi üstlerine düşen görevleri yerine getirebilecek yetkinlik, teknoloji ve yedeğe sahip olduklarından emin olmalı,
- En az bir adet Felaket Kurtarma Merkezi kurmalı,
- Yedekleme sürecini etkin işleyecek şekilde tasarlamalı ve alınan yedeklerin ek olarak Felaket Kurtarma Merkezi'ne iletilmesini sağlamalı,
- Felaket Kurtarma Merkezi içerisindeki cihazları, ağ bileşenlerini ve sistemleri, işin ana veri merkezi ile aynı şekilde veya minimumda iş etki analizi çıktılarını sağlayabilecek şekilde sürdürülebilmesini sağlayacak yapıda kurgulamalı,
- Kurtarma süresi hedefi (RTO) ve kurtarma noktası hedefini (RPO) her hizmet düzeyinde belirlemeli ve test etmelidir.

Felaket kurtarma planları, İş Sürekliliği Yönetimi ve BT Hizmet Sürekliliği Yönetimi uygulamalarının ana parçasını oluşturmaktadır. Organizasyonlar, bahse konu yönetim süreçlerinin idare edilmesi adına fonksiyonlar oluşturarak kurtarma planlarını belirlemeli ve işletilmesini sağlamalıdır. Etkin bir kurtarma planı aşağıdaki unsurları içermelidir:

- Tüm kritik iş uygulamalarını, BT hizmetlerini ve temel BT unsurlarını kapsamalı,
- Felakete müdahale yöntemlerini içermeli,
- Felaket durumu için rol ve sorumlulukları net şekilde belirtmeli, tedarikçi ve varsa diğer 3. partilerin sorumluluklarını da göz önünde bulundurmalı,
- Felaket anında, iletişimin kesintisiz sağlanması için ana haberleşme sürecini ve alternatiflerini içermeli,
- Kesinti sonrası yedeklerden dönüş sağlanması için gerekli aksiyonları kapsamalı,
- İş sürekliliği ya da diğer felaket kurtarma süreçleri ile ilişkilendirmeli,
- Büyük ölçekli sistem değişiklikleri doğrultusunda ve yılda en az bir kez olacak şekilde gözden geçirerek, gerekli ise güncellemelidir.

Felaket kurtarma testleri, çok yıllık planlar oluşturularak periyodik olarak gerçekleştirilmelidir. Kurtarma testleri gerçekleştirilirken özellikle kritik servisleri kapsayacak şekilde test planları hazırlanmalı, test sorumluları ve test senaryoları belirlenmelidir. Bu senaryolar felaket anının simülasyonu olacak şekilde tasarlanmalıdır. Testler için başarı kriterleri belirlenmeli ve test sonuçları, tatbikatlar sonrasında BT Hizmet Sürekliliği Yönetimi ve İş Sürekliliği Yönetimi fonksiyonları tarafından kontrol edilmelidir. Test sonuçlarının başarısız olması durumunda ise kurtarma planları gözden geçirilmeli ve gerekli iyileştirmeler kısa süre içerisinde gerçekleştirilmelidir.

Felaket kurtarma için net planları olan kuruluşlar, felaket durumlarının ardından daha hızlı bir şekilde eskiye dönebilecek ve durumdan dersler çıkararak gelişeceklerdir.

Sonuç olarak; BT Hizmet Sürekliliği Yönetimi, günlük kesintiler için planlama yapmakla ilgili değil, en kötü durum senaryolarını ele almak ve bunların gerçekleşmesi halinde müşterilerin ve çalışanların en az şekilde etkilenmesini sağlamakla ilgilidir.

2.6. Tedarikçi Riskleri ve Yönetimi

Tedarikçi riski, en geniş anlamıyla, tedarikçinin faaliyetleri, organizasyon yapısı ile kanun ve yönetmeliklere uyum düzeyi gibi hususlardan kaynaklanan olumsuzluklar sebebiyle hizmet/mal alan firmanın maruz kaldığı her türlü riski tanımlamaktadır.

Siber tehditler ve iklim riskleri gibi unsurlara kıyasla görece eski ve geleneksel bir risk kolu olarak konumlanan tedarikçi risklerinin önemi, son yıllarda gerek ülkeler gerekse şirketler nezdinde artış göstermiştir. Nitekim, özellikle 2019 yılının son çeyreğinden itibaren hayatımıza giren "COVID-19" salgını ile beraber, tedarikçi kaynaklı krizlerin sayısı, buna bağlı olarak söz konusu risklerin yönetimine atfedilen ilgi kayda değer şekilde artmıştır. Nitekim geride bıraktığımız dönemde, özellikle elektrikli araç üretimini derinden etkileyen "çip krizi", ülkeler arası ticareti durma noktasına getiren "konteyner krizi" ve Rusya-Ukrayna arasında sürmekte olan çatışmaların doğrudan ve dolaylı yansımaları olan "gıda krizi" ile "doğalgaz krizi" gibi arz sorunları, tedarikçi riskinin önemini yeniden risk ajandalarının üst sıralarına taşımıştır.

Aktarılan risklerin çözümüne yönelik olarak ülke ve şirketler tarafından alternatif ürün, rotasyon ve tedarikçilerin araştırılması gibi çok çeşitli aksiyonlar alınmıştır. Bugünün dünyasında ise, tedarikçi risklerinin yönetilmesi bir veya daha fazla sayıda ekosistemde aynı anda faaliyet gösteren şirketlerin operasyonlarını sorunsuz bir şekilde sürdürülebilmeleri adına hayati önem taşımaktadır.

Tedarikçi riskine maruz kalan, diğer bir ifadeyle dış kaynak kullanan firmaların çıkarlarını uygun şekilde korumak amacıyla, söz konusu risklerin yeterli şekilde değerlendirilmesi, azaltılması, kontrol edilmesi, olumsuz olaylar ya da fesih durumunda iş sürekliliğinin sağlanması için belirli ilkelere ve süreçlere uyulması gerekmektedir. Bu kapsamda ilgili risklere ilişkin olarak, "ISO 31000- Kurumsal Risk Yönetimi İlkeleri" içerisinde de açıklandığı üzere bu risklerin;

- Tanımlanması,
- Analiz Edilmesi / Ölçülmesi,

- Değerlendirilmesi,
- Azaltıcı Aksiyonların Alınması ve
- Kaydedilmesi, İzlenmesi ve Raporlanması

yerinde bir yaklaşım olacaktır.

Riskler

Hizmet alımı yapan şirketlerin karşılaştıkları tedarikçi kaynaklı riskleri, finansal ve finansal olmayan riskler başlıkları altında 2 kategoride gruplamak mümkündür.

Finansal riskler, tedarikçilerin mali bünyesindeki bozulmalar dolayısıyla mal ya da hizmet alımı yapan firmalara olan borçların vadesinde ya da beklenen kalitede yerine getirilememesini ifade etmektedir. Örneğin, faaliyetlerinin finansmanında yüksek düzeyde banka kredisi kullanan bir tedarikçinin kredi faizi oranlarındaki artışa bağlı olarak nakit akışının bozulması ve sağladığı hizmetin kesintiye uğraması olasıdır. Bu perspektiften, tedarikçilerin maruz kaldığı finansal risklerin kredi veren kuruluşlar veya bu hissedarlarının ötesinde, hizmet sağladıkları firmaları da etkileyebildiğini göz önünde bulundurmak önemlidir.

Öte yandan, finansal olmayan riskler başlığı altında faaliyet gösterilen sektör ve hizmet alınan konu özelinde de değişebilen çok sayıda riskin adını anmak mümkündür. Bu paralelde tedarikçi riski değerlendirirken firmaların;

- Sektördeki Konumu ve İtibarı (Sektör Tecrübesi, İnsan Kaynağı Havuzu vb.)
- Ortaklık ve Sermaye Yapısı (Güçlü Sermaye Yapısı, Ortak Moralitesi ve Tecrübesi)
- Risk Yönetimi Çerçevesi (İş Sürekliliği Planları, Siber Güvenlik Riskleri vb.)
- Uluslararası Yaptırımlar ve Suç Gelirlerinin Aklanması Mevzuatına Uyum Düzeyi
- ESG Konularına Uyum Seviyesi
- Diğer Kanun ve Yönetmeliklere Uyum Düzeyi

gibi unsurları asgari olarak göz önünde bulundurulmalıdır.

Son olarak, finansal olsun ya da olmasın tedarikçi kaynaklı her türlü riskin hizmet/mal alımı gerçekleştirilen işletmenin itibarını da zedeleyebileceği unutulmamalıdır.

Sonuç olarak, risk yönetim ilkeleri çerçevesinde faaliyet gösterilen sektör ve hizmet alınacak konu da göz önünde bulundurularak öncelikle mal/hizmet alımı yapan firma tarafından karşılaşılması muhtemel riskler tanımlanmalıdır. Risk yönetimi çerçevesi kapsamında alınabilecek aksiyonlara ilişkin önerilerimize izleyen bölümlerde, yer verilmektedir.

Risk Azaltımına İlişkin Kontrol Önerileri

Risklerin tanımlanması, analiz edilmesi ve değerlendirilmesi akabinde risk azaltımına ilişkin aksiyonlar üzerinde durulmalıdır. Bu bölümde ele alınacak başlıklar, "Yönetişim Çerçevesi" ve "Kontrol Yapısı" olarak ikiye başlığa ayrılmıştır.

Yönetişim Çerçevesi

Kurumsal Yönetim'in gereği olarak, tedarikçi risklerinin yönetimine ilişkin öncelikle bir yönetişim çerçevesi oluşturulması faydalı olacaktır. Tedarikçi riskinin yönetimine ilişkin söz konusu çerçevenin amacı, şirket içerisindeki rol ve sorumlulukların, riskin yönetimine ilişkin temel ilkelerin ve gözetim prensiplerinin belirlenerek şeffaf bir şekilde tüm paydaşlarla paylaşılmasıdır. Bu kapsamda;

- Şirket faaliyetlerinin; kilit faaliyet, önemli faaliyet ve basit faaliyet gibi başlıklar altında önem ve kritiklik düzeylerine göre sınıflandırılması,
- Söz konusu sınıflandırmaya bağlı kalınarak, şirketin dış kaynak kullanımına konu edebileceği/edemeyeceği faaliyetlerin açık bir şekilde listelenmesinin yanı sıra uyulması gereken asgari kıstasların bu sınıflandırma da gözetilerek ortaya konması,
- Tedarikçi seçimine ilişkin kriterlerin (fiyat-geçmiş tecrübeler-mali yapı vb.) hesap sorulabilirlik ilkesi çerçevesinde belirlenmesi,

- Yönetim Kurulu, İcra Kurulu, iş birimleri ve satın alma departmanı gibi paydaşların yetki ve sorumluluklarının açık bir şekilde belirlenmesi, bu kapsamda örneğin satın alım yetki limitlerinin ayrıştırılması,
- Yönetim Kurulu'nun gözetim rolü kapsamında, tedarikçi performanslarının ve tedarikçi risklerine ilişkin sürecin sağlıklı ve periyodik bir şekilde izlemesine olanak tanıyacak raporlama mekanizmalarının tesisi (satın alma komiteleri)
- İcra Kurulu ve İş Birimleri tarafından tedarikçilerin Servis Seviyesi (Service Level Agreement), Anahtar Performans ve Risk Göstergeleri (Key Performance and Risk Indicators (SLA,KPI,KRI) gibi performans metriklerinin takibinin sağlıklı bir şekilde yapılabilmesini yönelik altyapının tasarlanması,
- Çıkar çatışmasının önlenmesine yönelik olarak gerekli aksiyonların alınması, bu kapsamda örneğin tüm tedarikçi seçimlerinin asgari iki kişi tarafından onaylanması,
- Ölçek ekonomisinin getirilerinden faydalanmak üzere şirket genelindeki tüm satın almalar için merkezi bir satın alma birimi kurulması, ayrıca, grup şirketlerinin mevcut olması halinde, ölçek ekonomisinden faydalanmak üzere satın almaların grup nezdinde sürdürülmesinin sağlanması ve/veya bütünleşik bir satın alma süreci oluşturulması ve söz konusu prensiplerin tüm paydaşlarla rahatlıkla ulaşabileceği bir ortamda yazılı hale getirilmesi sağlanmalıdır.

Kontrol Yapısı

Yönetişim yapısının oluşturulmasını takiben yapılacak kontrollerin belirlenmesi tavsiye edilmektedir. Söz konusu kontrollerin;

- Sözleşme öncesi kontroller,
- Sözleşme süresince yapılacak kontroller

olmak üzere, 2 grupta sınıflandırılması anlamlıdır.

İş ilişkisinin kurulmasından önce yapılması gereken kontroller, tedarikçi adayı firmaların taahhütlerini beklenen kalite ve vade içerisinde yerine getirme kabiliyetini değerlendirmeyi hedeflemelidir. Bu kapsamda tedarikçi firma adaylarına ilişkin olarak;

- Firmanın, ortaklarının ve kilit yöneticilerinin herhangi bir uluslararası yaptırım listesinde olmadığının / MASAK mevzuatı kapsamında mal varlığının dondurulması da dahil olmak üzere kısıtlanmadıklarının teyit edilmesi,
- Risk yönetimi çerçevesinin anlaşılması, bu kapsamda; firmaların iş sürekliliği planlarının, risk/kontrol matrislerinin, iç denetim/kontrol raporları vb. temin edilmesi, gerekli görüldüğü hallerde saha ziyaretleri yapılması, ayrıca, kilit ya da önemli faaliyetler için daha sıkı kontroller talep edilmesi, ve
- Sözleşme kurulmadan önce SLA, KPI ve KRI'lar ile bunların arzu edilen seviyede bulunmaması durumunda alınacak aksiyonların kararlaştırılması, bu kapsamda çıkış planlarının oluşturularak alternatif tedarikçilerin belirlenmesi

tavsiye edilmektedir.

İş İlişkisi süresince;

- Yazılı sözleşmeler tahtında; veri gizliliği, fikri mülkiyet şartları, cezai şart ve fesih maddeleri ile SLA ve KPI'lar gibi tarafların borç ve yükümlülüklerinin açıkça belirlenmesi, bu yükümlülüklere uyulmadığı durumda uygulanabilecek yaptırımların sözleşmede yer alması,
- İzleme faaliyetleri kapsamında, KRI, KPI ve SLA'lerın belirli periyotlarla ve yakından takip edilmesi, belirlenen eşiklerin aşılması ya da yakalanamaması halinde önceden belirlenen aksiyon planlarının devreye alınması,
- Tedarikçinin kurum tarafından sağlanan hizmet kapsamında denetlenebilir olması,
- Tedarikçinin bilgi güvenliği ve iş sürekliliği çalışmaları kapsamında, tatbikat, gerçek olay veya krizlerde sorumluluklarını yerine getirebileceğinden emin olunması,
- Mümkünse tedarikçilerden alınan her bir hizmet için bir adet iş birimi sorumlusu bir adet de teknik sorumlu atanması, KRI, KPI ve SLA

gerçekleşmelerinin düzenli periyotlarla bu sorumlulara raporlanması, yılda bir veya daha sık bir periyotta tedarikçi memnuniyet anketlerinin ilgili sorumlular tarafından değerlendirilmesi,

- Firma ve ortakları hakkında yapılan yasaklı liste kontrolünün mümkünse güncel listeler ile her gün, bu mümkün değilse belirlenecek periyotlarla kontrol edilmesi,

İş ilişkisinin sona erdirilmek istenmesi ya da sona ermesini takiben ise;

- Çıkış planlarından da yararlanılarak, Hukuki, Operasyonel ve Veri Güvenliği konularına ilişkin alınacak aksiyonların ve yol haritasının belirlenmesi, çıkış süreci boyunca tedarikçiden hizmet alımına devam edilebilmesine yönelik önlem ve kontrollerin sağlanması, böylelikle, konunun şirket aleyhine açılabilecek davalar, operasyonel süreçlerin devamlılığı ve mevcutsa müşteri veri güvenliğine ilişkin unsurları kapsayacak şekilde çok boyutlu olarak paydaşlarla görüşülmesi önerilmektedir.

BÖLÜM 3

İŞLETME RİSKLERİNİN SİGORTACILIK VASITASIYLA DEVRİ

3. İŞLETME RİSKLERİNİN SİGORTACILIK VASITASIYLA DEVRİ

İşletmeler, faaliyet gösterdikleri dinamik iş dünyasında bir dizi belirsizlikle karşı karşıyadır. Bu belirsizlikler, sadece operasyonel sürekliliklerini etkilemekle kalmaz, aynı zamanda mali varlıklarını, çalışanlarını ve itibarlarını da tehdit edebilir. İlk bölümde, işletmelerin bu riskleri etkili bir şekilde yönetmek için kendi bünyelerinde risk yönetimi modelleri oluşturmalarının önemini vurgulamıştık. Bu bölümde ise, bu risklerin bir kısmını sigorta uygulamalarıyla devretmek üzerine odaklanacağız.

Sigorta, işletmelerin beklenmedik olaylara karşı finansal koruma sağlamak adına etkili bir araçtır. Ancak, sigorta uygulamalarından maksimum faydayı sağlayabilmek için doğru adımların atılması kritik bir öneme sahiptir. İkinci bölümde, işletmelerin doğru sigorta aracısını seçmeleri, sigortalanabilir varlıklarını belirleyip envanter oluşturmaları, doğru ürün ve teminatları belirlemeleri, fiyatlamaya etki eden faktörleri anlamaları, doğru teminat bedellerini belirlemeleri ve sigorta şirketleri ile etkili hasar yönetimi yapabilmeleri için izlemeleri gereken adımları ayrıntılı bir şekilde inceleyeceğiz.

Bu bölümde özellikle vurgulanacak konulardan biri, doğru teminatların belirlenmesi ve eksik sigorta kavramıdır. Çünkü işletmeler için uygun teminatları seçmek, bir riskin ortaya çıkması durumunda mali zararları en aza indirmek adına kritik bir rol oynar. Doğru bedelle teminatları oluşturmak ise işletmelerin karşılaşabileceği hasar durumunda sigorta ürünlerinden tam faydalanabilmeleri adına kritiktir. Bu noktada, işletmelerin karşılaştıkları riskleri mevcut ekonomik şartlar altında (kur dalgalanmaları, yerine koyma maliyetlerindeki artış vb.) değerlendirmeleri ve ardından bu risklere uygun teminatlar belirlemeleri, sigorta uygulamalarının etkili bir şekilde kullanılmasını sağlar.

Sigorta uygulamalarının doğru bir şekilde yönetilmesi, işletmelerin belirsizlikle başa çıkma yeteneklerini artırırken, aynı zamanda sürdürülebilir bir büyüme ve başarı için güçlü bir temel oluşturur.

3.1. Doğru Sigorta Aracısı Seçimi

İşletmeler, operasyon süreleri içerisinde çeşitli risklere maruz kalabilir ve bu riskler, işletmenin faaliyetlerini olumsuz etkileyebilir. İşletme sahipleri, bu riskleri minimize etmek veya yönetmek amacıyla çeşitli önlemler alabilirler. Bu önlemlerden biri de işletme risklerini sigortacılık aracılığıyla devretmektir. İşletme sahipleri, uygun bir sigorta aracısı seçerek işletme risklerini etkili bir şekilde yönetebilirler.

Uzmanlık ve Deneyim: Doğru sigorta aracısı, işletme sahibine özel ihtiyaçları anlayan ve sektörde deneyim sahibi olan bir profesyonel olmalıdır. İşletmenin karmaşıklığına ve özel risklerine uygun çözümler sunabilen bir aracı, işletmenin daha iyi korunmasını sağlar. Aracının danışmanlık ekipleri, sigortalı adayı için kapsamlı bir risk yönetimi planı çizerek, doğru riskleri transfer etmeleri konusunda yol gösterici olmalıdır.

Çeşitli Sigorta Ürünleri Sunabilme Yeteneği: İyi bir sigorta aracısı, işletmenin karşılaştığı çeşitli risklere karşı kapsamlı sigorta çözümleri sunabilme yeteneğine sahip olmalıdır. Yangın, hırsızlık, sorumluluk, Yönetici Sorumluluk, Siber Riskler vb. çeşitli riskler için uygun sigorta ürünlerini sağlayabilmelidir.

Güvenilir Sigorta Şirketleri ile İlişkiler: Doğru sigorta aracısı, güvenilir ve mali açıdan sağlam sigorta şirketleri ile iş birliği yapmalıdır. Bu, işletmenin poliçe taleplerini zamanında ve güvenilir bir şekilde yerine getirmeyi sağlar.

Kişisel İletişim ve İlgilenme: İyi bir sigorta aracısı, müşteri ile doğrudan iletişim kurabilen ve işletmenin değişen ihtiyaçlarına hızlı bir şekilde yanıt verebilen bir kişi olmalıdır. Kişisel ilgi, işletmenin güncel durumunu anlamak ve doğru sigorta çözümlerini önermek için önemlidir.

Rekabetçi Fiyatlandırma: Sigorta maliyetleri önemli bir faktördür. Doğru sigorta aracısı, işletmeye uygun sigorta çözümlerini rekabetçi fiyatlarla sunabilmelidir. Ancak, sadece düşük fiyat değil, aynı zamanda kapsamlı koruma da önemlidir.

Referans ve İncelemeler: Sigorta aracısının daha önceki müşterileriyle olan ilişkileri ve geri bildirimleri, onun hizmet kalitesi hakkında bilgi sağlayabilir. Referanslar ve online incelemeler aracılığıyla aracının geçmiş performansını değerlendirmek önemlidir.

Doğru sigorta aracısı seçimi, işletmenin sürdürülebilirliği ve başarısı için kritik bir faktördür. İyi bir aracı, işletmeyi olası risklere karşı etkili bir şekilde koruyabilir ve sigorta süreçlerini yönetmekte yardımcı olabilir.

3.2. Sigortalanabilir Varlıkların Belirlenmesi ve Envanteri

Sigortalanabilir menfaat ilkesi, teminat altına alınan rizikoların meydana gelmesi halinde, sigortalının mali açıdan kayba uğrama durumunda olmasını ifade eder. Sigortanın temel varsayımlarından hareketle sigortalanmak istenen varlıkların parasal olarak ifade edilebilir çıkarların, riskin gerçekleşmesiyle ortaya çıkan hasar durumunda sigortalının kayıplarının karşılanmasıdır. Bu menfaat hayat sigortası kapsamında can, kaza sigortaları kapsamında mal, sunulan hizmet kapsamında sorumluk şeklinde ortaya çıkabilir.

Riskin varlığı ekonomik birimlerin performansını etkiler ve bu yüzden kaynakların optimum tahsisine ve bütün ulusların ekonomik gelişimine kısıtlamalar getirir.

İşletmeler çok farklı nitelikteki çeşitli rizikolarla karşı karşıyadır. Bunlar yangın, yıldırım, infilak, doğal afetler, hırsızlık, kargaşalık, halk hareketleri, terör gibi doğrudan rizikolar ya da kâr kaybı gibi dolaylı nitelikte rizikolar olabilir. Ayrıca, çeşitli sorumluluklar gibi yasal rizikolar veya enflasyon gibi mali rizikolar da söz konusu olabilir.

Bu rizikolar karşısında İşletme Risk Yönetimi yoluyla önce işletmenin varlıklarını ve gelir sağlama kapasitesini hangi rizikoların tehdit ettiğini belirleyecek ve bu rizikoların gerçekleşme olasılıkları ile işletmeye olası etkilerini ortaya koyacaktır.

Risk yönetimi; riskin tanımlanması, ölçülmesi, değerlendirilmesi, sınırlandırmaya yönelik koruyucu önlemlerin alınması ve kontrol aşamalarından oluşmaktadır.

Risk yönetiminde ilk aşamada firmanın varlıkları ve sorumlulukları belirlenir. Firmanın dönen, duran varlıkları, borç ve öz sermayesinin yanlış belirlenmesi (eksik ve aşkın sigorta) sigortacı ya da sigortalının olumsuz etkilenmesine yol açabilir. Envanter çalışması olarak adlandırılabilecek bu çalışmaya firmanın fabrika binası, makineleri, taşıt araçları, yakıt depoları, hammadde-yarı mamul ve mamul depoları, büro malzemesi, iş durması kayıpları, üçüncü kişilere verilecek zararlar, hizmet sorumlulukları, yönetici kişilere verilecek zararlar, yönetici ve çalışanların sağlıkları vb. firma faaliyetlerinin niteliğine göre söz konusu varlık ve yükümlülük artabilir ya da azalabilir. Risk noktaları belirlendikten sonra bunların değerleri belirlenir. Değerlendirmede yerine koyma değerinin yanı sıra, fatura bedeli beyan esası araştırma ve ekspertiz değerleri kullanılmaktadır. Hasara uğrayan varlıkların yerine konması, pazar değeri üzerinden bir değerlendirme yapmayı gerektirir. Bu arada hasar nedeniyle firma faaliyetlerinin olumsuz etkilenmesi ve yükümlülüklerini yerine getirmemesinin sonuçları da hesaba katılmalıdır. Ayrıca poliçe süresince hasarın ortaya çıktığı zaman noktası da önemlidir. Zaman içindeki değer değişmeleri hesaba katılarak gerçek maliyetlerin belirlenmesi gerekir.

3.3. Doğru Ürün ve Teminatların Belirlenmesi

Sigorta ürünleri, sigortalılara sigorta sözleşmesinde belirtilen teminatlar ve limitler dahilinde güvence sunmaktadır. Sigortaya konu olan ve belirli bir prim üzerinden sigortalanan kişinin, eşyanın, aracın veya gayrimenkulün kısmen veya tamamen hasar alması sonucunda, hasarın sigorta poliçesi şartları dahilinde tazmin edileceği konusunda sigortacı kişinin sigortalı kişiye veya sigortadan menfaat sahibi olan kişiye verdiği güvenceye, "teminat" adı verilmektedir.

KOBİ'den endüstriyel işletmelere, atölyelerden üretim tesisleri ve ofislere, iş yerlerinin sektörel ve faaliyet kolu bazında farklılaşan risklerine ve ihtiyaçlarına özel hazırlanan ürün ve teminatlar ile işletmelere sigorta güvencesi sağlanmaktadır.

Söz konusu işletmeler çeşitli afetler, beklenmedik olaylar, hasarlar ve kazalar karşısında varlıklarını çok hızlı ve kolayca yitirebilmektedir. Aynı zamanda piyasalardaki olumsuz gelişmeler ve ekonomik krizlerden etkilenmektedir.

Sektörel poliçelere ait teminatları tek bir ürün içerisinde sunan, faaliyet grupları özelinde belirlenen ürün içerikleri ile işletmelerin ihtiyaçlarını karşılayacak paket ürünlerin yanı sıra fabrikalar gibi büyük çaplı işletmelere yönelik sigorta ürünleri de mevcuttur.

Sigorta poliçesi ile güvence altına alınan risk ya da risklerin gerçekleşmesi durumunda sigortacı kişi tarafından sigortalı kişiye ödenecek tutara "ana teminat" adı verilmektedir. Ancak sigorta yaptıran kişi, kendi ihtiyaçlarına uygun olarak seçebileceği ek teminat seçenekleri ile sigorta poliçesini genişletebilmektedir.

İşletmelerdeki binalardan mallara ve dekorasyona, makinelerden elektronik cihazlara ve işletme sorumluluğuna kadar tüm taşınır ile taşınmazlar sigortalının gereksinimlerine göre aşağıda belirtilen ana teminatların yanı sıra isteğe bağlı ek teminatlar / branşlar dahilinde poliçe teminatına dahil edilebilmektedir. Ayrıca her bir teminat için sigortacı tarafından poliçeye özel eklenmiş muafiyetler, şartlar veya notlar bulunabilir. Olası bir hasar sonrasında problem yaşamamak için teminatların poliçede yer alıp yer almadığının ve muafiyet oranlarının kontrol edilmesi önem arz etmektedir.

Yangın veya taşınmazlara bağlı ana ve ek teminatlar

- Yangın, Yıldırım, İnfilak
- Deprem
- Hırsızlık
- Kara, Deniz, Hava Taşıtları Çarpması
- Duman, Dahili Su, Sel, Su Baskını, Kar Ağırlığı, Yer Kayması, Fırtına
- Grev, Lokavt, Kargaşalık, Halk Hareketleri, Kötü Niyetli Hareketler ve Terör
- Cam Kırılması
- Dolu
- Kira Kaybı
- Kâr Kaybı
- Dolaylı İş Durması
- Alternatif İşyeri Değişikliği Masrafları
- Elektronik Cihaz

- Makine Kırılması
- Enkaz Kaldırma Masrafları

Sorumluluk ve diğer teminatlar

- Yangın Mali Sorumluluk
- Üçüncü Şahıslara Karşı Mali Sorumluluk
- Asansör Sorumluluk
- İşveren Mali Sorumluluk
- Ürün Sorumluluk
- Emniyet-i Suiistimal
- Taşınan Para
- Ferdi Kaza Sigortası
- Hukuksal Koruma

Yukarıda bahsi geçen yangın, kâr kaybı, deprem, hırsızlık, elektronik cihaz vb. gibi temel teminatlar klasik ürün gamında yaygın olarak sunulmaktadır. Bölüm 3.5'de işlenecek olan eksik sigorta kavramı ile birlikte değerlendirildiğinde işletmelerin sürekliliğini sağlamak için en temel teminatlardır. Bu temel teminatların yanında, koşullu kar kaybı, siber güvenlik, sorumluluk branşları altında verilen yönetici sorumluluk ve karşı taraf riskini teminat alında alan alacak sigortaları ise fiziki hasarların yanında özellikle son dönemde yükselişe geçen risklerin teminat altına alınması için kritik öneme sahip ürünlerdir. Bu ürünlerin tanıtımına kısaca aşağıda yer verilmiştir.

Kar Kaybı

Yangın, dahili su, terör ve benzeri olaylar ile deprem sel, fırtına ve yer kayması gibi doğal afetlerin oluşturduğu bu risklerin gerçekleşmesi durumunda birçok kaybın yanı sıra işletmenin kâr etme amacı da kesintiye uğrayacaktır. İş durması, üretim ya da hizmetin azalmasına ya da tamamen durmasına yol açar. Sonuçta, hasar olmasaydı elde edilmesi beklenen ciro azalır ya da hiç yapılamaz. Diğer yandan, sabit masrafların devam etmesi, kârın ve Pazar payının düşmesi, dolayısıyla öz sermayenin azalması kaçınılmaz olacaktır.

"Sabit Kıymet Sigortası" ile işletmenin sahip olduğu bina, fabrika, tesis, makine tesisat, emtia, demirbaş gibi mal varlıkları yangın ve diğer riskler sonucu meydana gelen maddi hasarlara karşı güvence altına alınır.

Ancak bu hasarın gerçekleşmesi nedeniyle işin durmasından doğacak kayıpları (ciro düşmesi, masraf artışı vb.) kar kaybı sigortası karşılar.

Yangına bağlı kâr kaybı sigortasında, hasarın meydana geldiği andan, ticari faaliyetin durma veya aksaması tamamen giderilerek normal faaliyete devam edilene kadar geçecek süre içinde, poliçede belirtilen şartlar çerçevesinde ve azami tazminat süresini aşmamak kaydıyla, meydana gelecek kâr kaybı ödenir.

Sigortacının sorumluluğu, sigorta poliçesinde belirtilen sigorta bedeliyle sınırlıdır. Sigortalı, hasar anında ticari faaliyetine imkanlar ölçüsünde devam ederek kâr kaybını önlemeye, azaltmaya ya da hafifletmeye yönelik önlemleri almakla yükümlüdür. Acil önlemlere ve sigortacı tarafından alınması istenilen önlemlere ilişkin giderler, sigortacı tarafından ödenir. Poliçede aksi kararlaştırılmadıkça sigorta bedeli brüt kardır.

Dolaylı İş Durması / Kâr Kaybı (Contingent Business Interruption)

İşletmelerin yönetmekte olduğu risklerin başında doğal olarak kendi bünyelerindeki fiziksel riskler gelmektedir. Ancak son birkaç yılda Dünya genelinde yaşanan pandemi, ticaret savaşları ve depremler gibi büyük coğrafyaları etkilemiş olaylar göstermiştir ki işletmeler sadece kendi risklerini yönetmekle kalmamalı aynı zamanda iş ilişkisinde bulundukları tedarikçilerin, kritik müşterilerinin veya kamu hizmetlerinin aksaması gibi riskleri de bertaraf etmelidirler.

Örneğin COVID-19 salgını, küresel çapta birçok işletmenin tedarik zincirini etkilemiş buna paralel olarak üretim tesislerinin kapanması, lojistik zorluklar, talep dalgalanmaları ve işgücü eksiklikleri, birçok sektörde tedarik zinciri sorunlarına yol açmıştır.

2011 yılında Japonya'da meydana gelen büyük deprem ve tsunaminin ardından, otomotiv ve elektronik sektörlerde faaliyet gösteren birçok uluslararası şirket, Japon

tedarikçilerinden malzeme temininde zorluklar yaşamış ve buna bağlı olarak kapasite azaltımı ve bazı üreticilerde iş durması yaşanmıştır.

Ukrayna önemli bir tarım ülkesi olarak bilinir ve özellikle tahıllar konusunda önemli bir ihracatçıdır. 2022 yılında Rusya'nın işgali ile fiziki çatışmaya dönüşen koşullar çatışmanın yoğunlaştığı bölgelerdeki tarım arazilerinin ve lojistiğin etkilenmesine neden olmuş, bu durum sektörde tedarik sorunlarına yol açmıştır.

Dolaylı iş durması teminatı sağlayan sigorta ürünleri, işletmelere; tedarik problemleri, kritik müşteri kayıpları, lojistik kesintiler, kamu otoritesinin müdahaleleri veya kamu hizmetlerinin kesintiye uğraması sonucunda ortaya çıkan iş durması ve kâr kayıplarını telafi eder. Bu yönüyle işletmenin kendi fiziksel risklerini teminat altına alan kâr kaybı ürünlerinin 360 derece tamamlayıcısı olarak konumlanmaktadır.

Siber Güvenlik Sigortası

Gerek gündelik gerekse kurumsal hayatta dijitalleşmenin hızlanması ve çoğu ihtiyacın online araçlar üzerinden giderilmesi siber suçlarda artışa neden olmaktadır.

Sigortalının bilgisayar sistemlerini olumsuz etkileyecek veya etkileme şüphesi bulunan her tür kötü niyetli fiili ya da insan hatası siber olay kapsamında değerlendirilir.

Siber riskler, maddi kayıpların yanı sıra özellikle şirketler için itibar kayıplarını da beraberinde getirmektedir.

Ticari Siber Güvenlik Sigortasında siber güvenlik riski nedeniyle oluşacak veri koruma hasarlarının yanı sıra siber saldırı sonrasında iş durması kaynaklı hasarlar, siber fidye hasarları, kişisel verilerle ilgili idari para cezaları, veri ihlali masrafları, bilgi güvenliği ve gizlilik sorumluluğu gibi riskler için poliçe koşulları dahilinde teminat sağlanmaktadır.

Yönetici Sorumluluk Sigortası

Kanun ve uygulamalar, yönetim kurulu üyeleri ve şirket yöneticileri için birçok yükümlülük getirmektedir. Yöneticilerin şirket içi ve dışı yönetimsel riskler altında yerine

getirdikleri görevler kapsamında ilgili kanunlarla yüklenen sorumlulukların ihlali ise, tazminat davası ve/veya cezai yaptırımla sonuçlanabilmektedir.

Bu çerçevede yöneticiler, bu yükümlülükler nedeniyle oluşan zararlardan şahsi olarak sorumlu tutulabilir ve şirket, şirket hissedarları, resmi devlet kurumları, şirket çalışanları, şirketin iş yaptığı firmalar, rakipler, alacaklı kurumlar, tasfiye memurları ve düzenleyici kurumlar tarafından dava edilebilirler.

Yönetici Sorumluluk Sigortası; yönetim, denetim kurulu üyeleri ve yöneticiler görevlerini yerine getirirken kötü niyet veya kasıt olmaksızın yaptıkları kusurlu eylemler, aldıkları hatalı kararlar ve ihmallere bağlı olarak neden oldukları zararlardan doğan yükümlülüklerini sigortalamaktadır. Şirketin, yöneticilerin uğradığı zararları karşılaması durumunda ise Yönetici Sorumluluk Sigortası poliçesi, şirketin yönetici adına katlandığı zararları şirkete ödemektedir.

Alacak Sigortası

Devlet desteğiyle sunulan Ticari Alacak Sigortası KOBİ'lerin yurt içi vadeli satışlardan doğan ticari alacaklarının ödenmemesi durumunda oluşan zararlarını karşılamaktadır. Devlet Destekli Ticari Alacak Sigortası'ndan basit usul dışında vergi mükellefi olan, başvuru tarihinden itibaren en az iki yıl önce kurulmuş olan ve yurt içi yıllık net satış hasılatı ya da mali bilançosu 500 Milyon TL'yi aşmayan, Özel Riskler Yönetim Merkezi tarafından belirlenen risk değerlendirme kriterlerini sağlayan KOBİ'ler yararlanabilir.

Bu sigorta sayesinde poliçe başlangıç tarihinden sonra yapılan sadece yurtiçi satışlardan doğan en fazla 360 gün vadeli ticari alacaklar teminat altına alınmaktadır.

Devlet Destekli Alacak Sigortasının işletmelere faydaları:

- Etkin alacak ve tahsilat yönetimi,
- Ticari alacaklara koruma,
- Güvenli ticaret imkânı ve
- Kredibilite

şeklinde sıralanabilir.

3.4. Sigorta Fiyatlamasına Etki Eden Faktörler

Sigortacılık teriminde fiyatlama, sigortacının üstlendiği riske karşılık sigortalı veya sigorta ettirenin prim ödeme yükümlülüğündeki satın alma fiyatı olarak tanımlanabilir. Yangın Sigortalarında fiyatlamaya etki eden ana faktörler; sigortalının ana faaliyet kolu, riski yönetmek için aldığı önlemler, işletmenin bulunduğu konumdaki doğal afet riskleri, sigorta poliçesinde yer alan teminatlar, bu teminatların limit ve muafiyetler olarak özetlenebilir. Bu noktalara ilave olarak sigorta şirketlerinin reasürans anlaşmaları, stratejileri ve risk kabul esasları da fiyatlamaya etki eden diğer önemli konulardandır.

Özellikle şiddet ve frekans açısından en sık görülen yangın riski değerlendirilirken, ilgili işletmenin faaliyet kolu, fiyatlamadaki ana etkendir. Kimya Mühendisleri Odası (KMO) İstanbul Şubesi'nin tespitlerine göre 2022 yılında, Türkiye'de 587 endüstriyel yangın hadisesi gerçekleşmiş olup; bu yangınların faaliyet kolu bazında ayrımına bakıldığında yangın yükü yüksek olan işletmelerde daha fazla olduğu görüldüğü belirtilmektedir. Frekans ve şiddetin yüksek olduğu bu tip işletmeler ve diğer bütün işletmelerde, ilgili risklerin bertaraf edilmesi için alınan önlemler ve işletmenin risk yönetimi hem poliçe yapılması hem de fiyatlandırılmasında çok büyük rol oynamaktadır. Bu raporun "2.1 Temel Yangın Risk Yönetimi" bölümünde de üzerinde durulan; işletmelerin alacağı önlemlere göre sigorta şirkleri kendi bünyelerindeki risk mühendisleri ile saha ziyaretleri yaparak faaliyet kolu, alınan önlemler ve işletmenin risk iştahını değerlendirmektedir. Ayrıca riskin bertaraf edilmesi için işletmelere danışmanlık vermektedirler. Bu değerlendirme akabinde poliçe primi belirlenmektedir. Risk yönetimi iyi olmayan, kendi faaliyet koluna göre gerekli önlemleri bulunmayan ve işletmelerine bu kapsamda yatırım yapmayan sigortalıların teminat bulmada veya uygun fiyatla teminat bulmada dönem dönem güçlük çektikleri gözlemlenmektedir.

Yangın sigortalarında fiyatlamaya etki eden diğer bir konuda da deprem başta olmak üzere ilgili rizikonun bulunduğu konumun doğal afet riskidir. Deprem riski için Sigortacılık ve Özel Emeklilik Düzenleme ve Denetleme Kurumu (SEDDK) tarafından yayınlanan "İhtiyari Deprem Tarifesinde" yer alan fiyatlamalar kullanılmaktadır. Bu

fiyatlamada risk adresi dışındaki diğer bir önemli konu ise deprem teminatında kullanılan muafiyet oranlarıdır. Sigortalının kendi mali bünyelerini düşünerek muafiyet oranlarını yükselterek (riskin bir kısmını kendi bünyelerinde tutmaları) fiyatlamalarda farklı indirimlerden yararlanması mümkündür. Deprem dışında teminat alınan sel/seylap, yer kayması vb. doğal afetler de günümüzde "İkincil Afetler" olarak tanımlanmış olup, fiyatlandırmaya etki eden diğer faktörler arasında yer almaktadır.

Sigorta ürünlerinin fiyatlaması, ülkemizde ve dünya genelinde meydana gelen doğal afetler ve büyük hasarlar gibi olaylardan etkilenebilmektedir. İçinde bulunduğumuz dönemde, iklim krizinin bir sonucu olarak, dünya genelinde ve Türkiye'de katastrofik riskler sigorta sektörü üzerinde maliyet baskısı yaratmakta bunun sonucu olarak ürün fiyatlarında artış gözlemlenmektedir. 2023 yılı özelinde ülkemizde yaşanan 6 Şubat Kahramanmaraş depremi ve devamındaki sel olayları, sigorta sektörünün en önemli maliyet kalemlerinden biri olan reasürans fiyatlarını önemli ölçüde artırmıştır. Bu raporun "2.1 Temel Yangın Risk Yönetimi" bölümünde vurgulanan önlemlerin alınması, sigortalıların artan sigorta maliyetlerini yönetmelerinde önemli bir faktördür.

3.5. Doğru Teminat Bedellerinin Belirlenmesi ve Eksik/Aşkın Sigorta

Sigorta poliçelerinde en çok dikkat edilmesi gereken konulardan bir tanesi, poliçelerin doğru bedelden düzenlenerek hasar sırasında eksik/aşkın sigortaya uygulamalarından korunmaktır. 6 Şubat Kahramanmaraş depreminde sigortalıların en çok mağduriyet yaşadığı konulardan bir tanesi de eksik sigorta bedelleri sebebiyle hasarların tenzil edilerek ödenmesi olmuştur. Bu durum sigortacılar için ise maalesef hasar süreçlerinde sorun ve güvensizlik algısına neden olmaktadır.

Yangın poliçelerinde sigorta bedeli aksi belirtmediği sürece rayiç bedel üzerinden belirlenir. Rayiç bedel en basit anlatım ile bir malın piyasadaki o anki kullanım durumu gözetilerek belirlenmiş güncel değeridir. Bu bedel binalarda binanın yeniden inşa edilmesi maliyetinden her yıl yaklaşık 2-3% amortisman payı düşülerek hesaplanırken, muhteviyat bedeli ise sigortalı tarafından beyan edilmektedir. Emtea bedeli belirlenirken emtea stoğunun maksimuma ulaştığı veya ulaşması muhtemel bedeli esas alınabilir. Emtea

bedelinin sıkça değiştiği durumlarda ise düzenli bildirim esaslı "Yangın Abonman" poliçeleri de düzenlenebilmektedir. Bu sigorta türü, sigortalının sigorta vadesi içinde elinde bulunabilecek azami emtea miktarını tespit ederek bu meblağ üzerinden bir abonman poliçesi düzenlenmesi ve ardından belirli periyodlarla günlük stoklarını sigorta şirketine bildirmesi şeklinde işler. Sigorta şirketi azami miktardan (meblağdan) poliçe kestiği zaman peşin olarak o meblağın ve karşılığı olan primin %40'ını alır. Daha sonra sigortalının aylık ya da üç aylık mevcut bildirimlerine göre de mevcutların peşin alınan %40'ı geçtiği miktar için fark prim talep eder. Mevcutlar %40'ın altında kaldığı takdirde herhangi bir prim veya iadesi söz konusu olmamaktadır.

Sigortalı tesisin yeni yapılmış olması durumunda, sigorta ettiren ve sigortacı poliçenin yeni değer (yeniye ikame) üzerinden yapılması konusunda anlaşabilirler. Bu durumda, poliçenin ikame bedeli (yeni değer) üzerinden tanzim edildiği poliçe notlarına açıkça yazılmalıdır. Yeni değer (nakliye, montaj, gümrük, vergi, resim, harç masrafları dâhil olmak üzere yenisinin ikame bedeli) esasına göre tanzim edilen poliçelerde, teminat kapsamına dahil edilmiş olan kıymetlerin tazminat ödemelerinde;

a) Poliçede eskime, aşınma, yıpranma (kullanma) payı için poliçede belirtilmiş olan oranın veya yaşın aşılmaması kaydıyla, rizikonun gerçekleştiği yer ve tarihte sigorta konusu kıymetin yeniden yapım veya alım maliyetine göre bulunan ikame bedeli esas alınır. Fakat, sigortacının eksik sigorta, sovtaj ve belirgin teknoloji farkından kaynaklanan tenzilat hakları saklıdır.
b) Eskime, aşınma ve yıpranma (kullanma) payı için poliçede belirtilmiş olan oranının veya yaşın aşılmış olması halinde, tazmin belirlenmesinde rayiç bedel dikkate alınır.

Sigorta poliçesinin yapılması sırasında ya da sigorta vadesi içerisinde, sigortalı ve sigortacı poliçe bedellerini (ticari mallar hariç) belirlemek üzere bir aracı kurum ile anlaşabilirler. Ardından, bilirkişi tarafından mutabakatlı kıymet takdir raporu hazırlanır ve sigortalı taraflara sunulur. Her iki tarafın da bu rapordaki bedeller üzerinden anlaşması durumunda, poliçe bedelleri güncellenerek poliçeye "mutabakatlı kıymet esasına göre tanzim edilmiştir" notu eklenir ve mutabakat raporu tarihinden itibaren meydana gelecek hasarlarda, eksik/aşkın sigorta uygulaması yapılmaz. Bu raporlar en çok 1 yıl için geçerli

olup, poliçelerin TL olması ya da enflasyonun yüksek olduğu senelerde, 1 yıllı süre dolmadan, tarafların anlaşmalarına paralel olarak güncellenebilir.

Eksik /Aşkın Sigorta

Poliçe sigorta bedellerinin yukarıda belirtilen standartlara uyulmadan düzenlendiği durumlarda, bir hasar anında eksik/aşkın sigorta hükümleri geçerli olmaktadır. Eksik sigorta, poliçede belirtilen sigorta bedelinin hasar anındaki sigorta değerinden daha düşük olması durumunu ifade etmektedir. Eksik sigorta olması durumunda Türk Ticaret Kanunu'nda belirtilen orantı kuralına göre sigortacının ödeme yapması gereken tutar hesaplanır. Örneğin; hasar tarihinde sigorta değeri 1.000.000 TL olan bir malın, poliçedeki sigorta bedeli 500.000 TL olduğu bir durumda, bir hasar sonucu oluşan hasar tutarının 200.000 TL ise orantı kuralına göre sigortacının azami ödeyeceği tutar 100.000 TL olmaktadır.

Özellikle; yüksek enflasyon yaşanan ekonomik durumlarda, yapı maliyetlerinin hızlı artması, ithal edilen makine/tesisat gibi varlıkların fiyatlarındaki kur dalgalanmaları, emtea fiyatlarındaki yüksek artış vb. sebepleri ile eksik sigorta riski oldukça artmaktadır. Bu sebeple poliçe bedelleri belirlenirken başta sigorta aracıları olmak üzere bu konuda uzman profesyonellerden destek alınması oldukça kritiktir.

Diğer taraftan vade başında doğru bedelden düzenlenen poliçeler, yine vade süresinde enflasyon ya da kur dalgalanmalarına karşı eksik sigorta riski ile karşı karşıya kalabilirler. Bu tip değişken ekonomik şartlarda poliçe içerisinde "Enflasyon Koruma Klozu" ve "Eksik Sigorta Koruma" klozlarının bulunması özellikle TL üzerinden yapılan poliçelerde ilave korumalar sunmaktadır. Ayrıca yıl içerisinde bedellerin düzenli olarak kontrol edilerek bu konuda sigorta aracılarından ve konu uzmanlarından destek alınması eksik sigorta riskini önemli ölçüde azaltacaktır. Ancak buradaki önemli konu, poliçenin vade başında mutlaka doğru bedeller üzerinden hazırlanmış olmasıdır.

Aşkın sigorta ise sigortalanan varlığın sigorta bedelinin, sigorta değerinden fazla olması durumudur, kısaca eksik sigortanın tam tersi durumdur ve ilgili TTK maddesine

göre bedelin aşkın olan kısmı geçersizdir. Hasar anında aşkın sigorta tespit edilmesi durumunda; hasar poliçede belirtilen bedel üzerinden değil malın gerçek değeri üzerinden ödenir. Aşkın sigorta olarak tespit edilen poliçelerde, sigorta şirketi poliçe iptaline gidebilir.

Belirtilen bilgiler ışığında özellikle yüksek enflasyon ve kur dalgalanmalarının yaşandığı dönemlerde doğru bedeller üzerinden sigorta poliçesi düzenlenmesi hasar anında eksik sigorta uygulamalarından kaçınmak için çok önem taşımaktadır. Sigorta programlarında doğru teminat bedellerinin belirlenmesi için kısaca aşağıdaki adımlar takip edilebilir:

- Poliçe bedeli aksi belirtilmediği sürece rayiç bedelden düzenlenmelidir. Yeni bedelden tazmin edilmesi durumunda poliçeye mutlaka açıkça not edilmelidir.
- Poliçe bedelleri altta belirtilen maddeler dikkate alınmalıdır:
    - Bina bedeli; binanın yeniden inşa edilmesi maliyetinden her yıl yaklaşık 2-3% amortisman payı düşülerek hesaplanır. Bina sigorta bedelinin tespitinde arsa bedeli dikkate alınmaz.
    - Emtea: Bir poliçe döneminde (1 yıl) emtea stoğunun maksimuma ulaştığı veya ulaşması muhtemel bedelidir.
    - Demirbaş: Riziko adresinde bulunan ve resmi defterlere demirbaş adı altında kayıtlı olan taşınabilir değerlerdir.
- Makine riziko adresinde bulunan ve sigortalımızın ticari faaliyeti içerisinde kullandığı ağırlıklı olarak mekanik aksamlı çalışan makinalar dahil mekanik aksamlı tüm makine ve tesislerdir. Doğru bedeller üzerinden tanzim edilen poliçelerde yıl içerisindeki enflasyon ve kur dalgalanmalarına karşı "Enflasyon Koruma Klozu" ve "Eksik Sigorta Koruma Klozu" eklenmelidir.
- Belirli aralıklar ile (örn. 3 ayda bir) bedellerin kontrol edilmesi ve gerekli olduğu durumlarda poliçelere ek belge ile teminat bedeli düzeltilmelidir.

3.6. Sigorta Şirketleri ile Hasar Yönetimi

İşletmelerde riskin tanımlanması, uygun yöntemlerle yönetilmesi ile sigortacı ve aracılarının hem risk mühendisliği vasıtasıyla risklerin tespit ve yönetiminde hem de uygun sigorta sözleşmeleri ile risklerin transfer edilmesinde yarattığı katma değer

önemlidir. Tüm bu süreçlerin en iyi şekilde yönetildiği durumda dahi riskler gerçekleşebilmektedir. Risklerin önceden transfer edilmesi durumunda işleyecek sigorta mekanizması, sigortalıların operasyonlarının bir an önce devam edebilmesi için gerekli aksiyonlarının alınması için harekete geçecektir. Bu süreçte, hasar anında sigorta değerinin doğru olup olmadığı ve bu sebeple oluşabilecek hasar tenzilatlarının önüne geçebilmek için, poliçeler yapılırken ve yapıldıktan sonraki süreçte, sigorta bedelinin bir önceki bölümde detaylandırıldığı şekilde dikkatlice değerlendirilerek güncel olması büyük öneme sahiptir.

Bu doğrultuda sigorta bedelinin ana kalemlerini oluşturan kıymetlerin bedellerinin; kur dalgalanması, dünya genelindeki enflasyonist ortam gibi çeşitli sebeplerle fiyat değişikliği yaşadığı dönemlerde, sık aralıklarla gözden geçirilmesi tavsiye edilmektedir. Eksik bedel ile sigortalanmış bir kıymet, karşılaşılabilecek olası hasarlar sonrasında da bu bedeller üzerinden değerlendirileceğinden şirketlerin bu konuya dikkat etmeleri yararlı olacaktır.


TÜSİAD