Kritik Altyapılarda Siber Risk Analizi ve Yönetimi

Cyber Risk Analysis and Management for Critical Infrastructures

Emre KIRAN
Gebze Teknik Üniversitesi
Bilgisayar Mühendisliği Bölümü
emrekiran@gtu.edu.tr
ORCID:0000-0003-2511-5579

İbrahim SOĞUKPINAR
Gebze Teknik Üniversitesi
Bilgisayar Mühendisliği Bölümü
ispinar@gtu.edu.tr
ORCID: 0000-0002-0408-0277

Öz

İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünü kritik altyapı olarak değerlendirmektedir. Bahse konu yapıların hayati önemi nedeniyle korunması ve korunabilmesi için de öncelikle değerinin bilinmesi ve hangi risklere maruz olduğunun tespiti gereklidir. Bu kapsamda yapılacak çalışmalar risk analizi olarak değerlendirilmekte olup, risk analizi kritik altyapının bozulmasının ya da yıkımının olası etkileri ile zayıf noktalarını değerlendirebilmek için ilgili tehdit senaryolarının göz önünde bulundurulmasıdır. Konunun öneminin gün geçtikçe artması nedeniyle hem ülkeler hem de uluslararası kuruluşlar tarafından standartların belirlenmesi, koruma çerçeveleri oluşturulması çalışmaları hız kazanmıştır. Bu çalışmada uluslararası standart ve çerçevelerden faydalanarak kritik altyapıların korunması, risk analizi ve yönetiminin yapılmasına yönelik bir çatı önerilmiştir.

Anahtar Sözcükler *- Risk Analizi, Kritik Altyapılar, Katmanlı Mimari, Senaryo Tabanlı Yaklaşım, Risk Yönetim Standartları, Perspektif Risk Yaklaşımı*

Abstract

As a result of the negative impact of the environment, the social order and the public services when it fails to fulfill its function partially or completely, it considers the network, assets, systems and structures that will have a serious impact on the health, safety and economy of the citizens as a critical infrastructure. In order to protect these buildings due to their vital importance, it is necessary to know the value and to determine which risks they are exposed to. The studies to be carried out in this scope are considered as risk analysis that is to take into account the related threat scenarios in order to evaluate the possible effects and weaknesses of the degradation or destruction of the critical infrastructure. As the importance of the issue has increased day by day, efforts have been accelerated by both countries and international organizations to set standards and to establish protection frameworks. In this work, a framework is proposed to form for the protection of critical infrastructures, risk analysis and management by making use of international standards and frameworks.

Keywords *- Risk Analysis, Critical Infrastructures, Layered Architecture, Scenario-Based Approach, Risk Management Standards, Perspective Risk Approach*

Gönderme ve kabul tarihi: 22.11.2019- 29.03.2020
Makale türü: Araştırma

1. Giriş

Son yıllarda meydana gelen siber saldırı ve olaylar ile yaşanan doğal afetler birçok ülke ile birlikte küresel ve bölgesel kuruluşu güvenlik kavramını tekrar gözden geçirmeye zorlamıştır. Gerçekleşen siber saldırıların amaçları bakımından politik, sosyo-kültürel ve ekonomik [1] olmak üzere üç alanda yoğunlaştığı ve bu alanlardaki kesişim noktasının,

diğer bir deyişle tüm alanlarda etki yaratacak bir saldırının kritik altyapılara yönelik olması gerektiği görülmüştür. Yaşanan her saldırı, olay ve doğal afet ülkelerin güvenliği ve vatandaşların refahı açısından önemli altyapıların belirlenmesi ve korunmasının gerekliliği konusunda ciddi bir görüş birliğinin oluşmasına yol açmıştır. AB Komisyonunun hazırlamış olduğu 2004 tarihli, 702 sayılı ve "Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması" başlıklı tebliğde [2] "Kritik altyapı" "İnsanların hayati sosyal fonksiyonlarının, sağlıklarının, emniyetlerinin, güvenliklerinin, ekonomik ve toplumsal refahlarının devamı için gerekli olan ve aksama veya yok edilmesi bu fonksiyonları sürdürmede yetersiz kalma sonucunda bir üye ülkede belirgin etki gösterecek varlık, sistem veya ilgili parçaları" şeklinde tanımlanmıştır. ABD mevzuatında "kritik altyapı" tanımı; "ABD için hayati fiziksel veya sanal sistemler ve varlıklar öyle ki böyle sistemlerin ve varlıkların kapasitesiz bırakılması veya yok edilmesi güvenlik, ulusal ekonomik güvenlik, ulusal kamu sağlığı veya emniyeti veya bütün bu sayılanların bir birleşimi üzerinde zayıflatıcı etkiye sahip olacaktır." şeklindedir [3].

Kritik altyapılar ile ilgili tanımlara bakıldığında toplumsal düzenin ve kamu hizmetlerinin devamlılığının sağlanmasının esas alındığı görülmektedir. Bu noktadan hareketle, kritik altyapılar daha kapsayıcı olarak; "İşlevlerini, kısmen veya tamamen, yerine getiremediğinde, toplumsal düzenin sürdürülebilirliğinin ve/veya kamu hizmetlerinin sunumunun olumsuz etkileneceği ağ, varlık, sistem ve yapılar bütünü" şeklinde tanımlanabileceği değerlendirilmektedir. Kritik altyapıların tanımı gibi kapsamı da ülkeden ülkeye değişmektedir. ABD hükümeti kritik altyapıların korunması çalışmalarını Ulusal Güvenlik kapsamında değerlendirmiş ve kritik altyapıları "Ulusal Altyapı Koruma Planı" ile belirlemiştir. AB'nin kritik altyapıların korunmasına bakışı ABD'ye nazaran farklılık arz etmektedir. AB bu konuya üye ülkelerinde ikamet eden vatandaşların sağlık, emniyet, güvenlik ve ekonomik refahı ile üye ülke hükümetlerinin etkin işleyişinin korunması açısından bakmaktadır.

Ülkemizdeki kritik altyapıların korunması çalışmaları incelenecek olursa, önümüzdeki yıllarda hazırlanması muhtemel siber güvenlik stratejilerinin, dolayısıyla ulusal seviyedeki siber güvenlik çalışmalarının ana temasının "kritik altyapıların korunması" olacağı değerlendirilmektedir. Bu kapsamda ülkemizde yapılan en önemli çalışmaların başında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı ve 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi [4] gelmektedir. Gerek strateji belgesinin amacı ve kapsamı gerekse 29 adet eylem maddesi çok büyük oranda "kritik altyapıların korunması" temasının altını doldurmaktadır. Bununla birlikte kritik altyapıların önemini Şekil–1'de yer alan görselle ifade eden AFAD'ın koordinasyonunda hazırlanan 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi'nde [5] "Son yıllarda artan terör tehdidiyle ve yaşanan büyük çaplı felaketler ülkeleri kritik altyapıların korunmasıyla ilgili politika, strateji, mevzuat, plan ve programlar yapmaya itmektedir" denilmiştir.

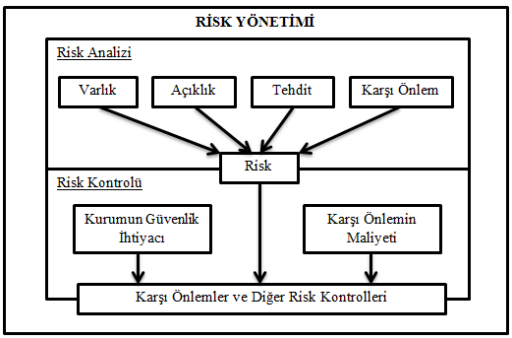
Kritik altyapı kavramının ortaya çıkmasının en önemli nedeni bilgi teknolojilerinin yaygın bir şekilde kullanılmasıdır. Toplumsal yaşamda birçok altyapının temeli/sürdürülmesi kritik altyapılara bağlı olduğu gibi, bilgi çağında kritik altyapıların temelinde de siber/bilişim altyapıları yer almaktadır [6][7]. Kritik altyapılar ve bilgi teknolojileri birçok yönden ve ciddi şekilde kesişmektedir. Bu kesişimler bilgi teknolojilerinin önemini çok açık bir şekilde göstermektedir. Bu önem, "kritik bilgi altyapıları" teriminin ortaya çıkmasına yol açmıştır. OECD, kritik bilgi altyapılarını, fonksiyonelliğini yitirmesi durumunda sağlık hizmetlerine, toplumsal emniyet ve güvenliğe, vatandaşların ekonomik refahına veya hükümetin/ekonominin verimli çalışmasına ciddi yönde tesir eden bilgi ağları ve sistemleri olarak tanımlamaktadır [8]. Bu kapsamda gerçekleştirilen çalışma kritik altyapıların temelini teşkil eden kritik bilgi altyapılarına odaklanmıştır.

Şekil – 1: Kritik Altyapılar [5]

Ulusal ve uluslararası alanda en üst düzeyde yürütülen kritik altyapıların korunması çalışmalarının en önemli adımlarından birisi faaliyet alanına giren sistemde bulunan varlıkları, varlıklardaki açıklıkları,

açıklıklarda kullanılabilecek tehditleri ve varlığı korumak için kullanılan güvenlik önlemlerini ortaya konmasıdır, yani risk analizi ve yönetimidir. Bilgi güvenliğine yönelik standartlarda da [9][10] bilgi güvenliği yönetim sisteminin ilk adımı olarak güvenlik politikasının tanımlanması ve risk yönetimi olduğu belirtilmiş ve varlıklara yönelik risklerin belirlenmesi ve bu risklere karşı önlem alınması bilgi güvenliği yönetiminin en önemli adımını teşkil ettiği vurgulanmıştır.

Bir varlıktaki açıklığın bir tehdit tarafından kötüye kullanılma ihtimaline risk denmektedir. Mutlak güvenlik olmadığından dolayı varlığı etkileyen riskler her zaman olacaktır. Bu kapsamda bir varlıktaki riskleri ortaya koyan, yorumlayan, risklerin verebileceği zararı kestiren ve ortaya konan risk senaryosuna göre faaliyetler yapan bir yapıya ihtiyaç vardır ve bu yapıda Şekil–2'de gösterilen risk yönetimidir.



Şekil – 2: Risk Yönetimi

Risk yönetim yapısı iki alt bileşenden oluşmaktadır: Risk Analizi ve Risk Kontrolü. Risk analiz sürecinde nitel ve nicel yöntemler vardır. Nicel risk analiz yöntemlerinde matematiksel ve istatistiksel yöntemler ile sayılar kullanılır. Bu yöntemler arasında risk tabloları, bulanık mantık, hata ağaçları, girdi–çıktı analizi ve benzetim vardır. Nitel risk analiz yöntemlerinde riski ifade etmek amacıyla sayılar, formüller, denklemler yerine az, çok, yüksek gibi sıfatlar kullanılır. Nitel risk analiz yöntemleri önceliklendirmede başarılı ve nicel yöntemlere göre daha hızlı olmakla beraber sayısal değer vermemekte ve maliyet analizi yapılması zor olmaktadır. Nicel yöntemlerde olumsuz etkilerin ölçüleri bağımsız olarak elde edilebilmektedir. Ayrıca parasal hesaplamalar ve bütçe belirleme gibi hususları mümkün kılar. Ancak hesaplama açısından yavaş, daha maliyetli ve büyük ölçüdeki verilerin toplanmasını gerektirir.

Bahse konu yöntemler zaman içerisinde özelleşmiş ve kabul görerek uluslararası standartlar haline dönüşmüştür. Bu kapsamda yayımlanan standartlar; ISO 31010 Risk Değerlendirme Teknikleri [11] ve ANSI 7690.3 Risk Değerlendirme Teknikleri [12] standartlarıdır. Standartlarda belirlenen teknikler kontrol, istatistik, senaryo analizi, destek, fonksiyon analizi vb. yöntemler olarak gruplanabilmekte ve organizasyonun yapısına göre uygun karakterde teknik organizasyon varlıklarına uygulanabilmektedir.

Belirtilen teknikler tek başlarına bir varlık/organizasyonun risk analiz/yönetimini gerçekleştirmede yeterli olmayacaktır. Bu kapsamda risk analiz/yönetimine yönelik CRAMM [13], COBRA [14], ISRAM [15], OCTAVE [16], RAMEX [17], TUAR [18] vb. bahse konu teknikleri kullanan birçok yöntem geliştirilmiştir. Bu yöntemler genel çerçevede değerlendirmeler sunmakta olup birçok farklı yapının analizinde kullanılmış [19][20] ve kıyaslamalarına yönelik çalışmalar [21] yapılmıştır. Bununla birlikte ISO 31000 Risk Yönetim Süreci Modeli [22], ISO 27005 Bilgi Güvenliği Risk Yönetim Standardı [23] ve NIST 800-39 Bilgi Güvenliği Risk Yönetim Standardı [24] gibi uluslararası standartlarda belirlenmiştir.

Yukarıda belirtilen tüm çalışmalar Risk Analiz ve Yönetiminde en kabul görmüş, birçok yöntem/teknik/standart/model/çerçevenin temelini teşkil eden Varlık – Açıklık – Tehdit yapısı üzerine oturmakta olup kritik altyapıların korunmasına yönelik birçok çalışma olmasına rağmen risk analiz ve yönetim konusunda bahse konu yapıları kavramlarının temeline koyan çalışmalar değillerdir. Bu kapsamda literatürde yapılmış ve kabul görmüş birçok yöntem/teknik/standart/model/çerçeve irdelenerek kritik altyapıların korunmasına yönelik en önemli adımlardan birine yönelik bir çerçeve tasarımı oluşturulmuştur.

Makalenin sonraki bölümlerinin yapısında, konu üzerindeki çalışmalar Bölüm 2'de, önerilen çatı Bölüm 3'de, vaka çalışması ve değerlendirme Bölüm 4'de verilmiştir. Bölüm 5 sonuç ve önerilerdir.

2. İlgili Çalışmalar

Kritik altyapılar üzerinde literatürdeki risk analizi ve yönetimi çalışmaları irdelenecek olursa; çalışmaların, Kritik Altyapıların geneli üzerinde yapılan risk analiz ve yönetim çalışmaları ile Kritik Altyapıları oluşturan varlıklar üzerinde yapılan risk analiz ve yönetim

çalışmaları gibi iki alanda odaklandığı görülecektir. Bu çalışmada, her iki çalışma alanının yetersiz geldiği konular üzerinde analiz yapıldığı gibi güçlü olduğu değerlendirilen ve birbirini tamamlaması gereken hususlarda değerlendirilerek ortaya konan tasarımın çatısı oluşturulmuştur.

Risk analizi ve yönetimi çalışmaları kapsamında literatürdeki en kabul görmüş yöntem olarak varlık – açıklık–tehdit modeli görülmektedir. Tabii ki burada varlık değerlendirmesi göreceli bir kavram olmaktadır. Yani değerlendirme seviyesi, yapılan değerlendirme türüne göre değişkenlik göstermektedir. Kritik altyapıların geneli üzerinde yapılan değerlendirmelerden kasıt, varlık olarak kritik altyapının kendisini gören çalışmalardır. Bahse konu çalışmaların en olumsuz olarak değerlendirilebilecek yönü de budur. Çünkü devletler, organizasyonlar, kurumlar, şirketler, akademik kuruluşlar vb. tarafından konu üzerinde yapılan çalışmalar incelendiğinde kritik altyapılara verilen önem açık bir şekilde ortaya konmaktadır. Dolayısıyla hassas bir yapı üzerinde yapılacak değerlendirmelerin de hassas olması gerekmektedir. Bu hassasiyeti sağlamak amacıyla da yapılacak değerlendirmelerin olabildiğince derinine uygulanması gerekmektedir. Belirtilen odak noktası üzerinde yoğunlaşan çalışmalardan ön plana çıkanlarının genel bir değerlendirmesi bölümün bundan sonraki kısımlarında verilmektedir.

Bagheri ve Ghorbani, perspektif yaklaşımlarla senaryo üretimine dayalı çalışmasındaki [25] yaklaşımın dolaylı etkileri göz ardı eden eksik yönlerinin giderilmesi durumunda kritik altyapılar üzerinde yapılacak değerlendirmede önemli bir boşluğu doldurabileceği değerlendirilmektedir. Burada ihtiyaç duyulacak senaryo üretimi risk değerlendirmesinde hassasiyeti sağlamak adına derinine yapılan irdelemelerin sonuçlarının üst seviyelere aktarılmasında kullanılacaktır. Buradaki dolaylı etki eksikliğinden kasıt genel kabul görmüş ve üzerine birçok kuram geliştirilmiş bir olayın başka olayları tetiklemesi yaklaşımıyla doğru orantılıdır. Kurulacak tasarımda her bir adım diğer adımları etkileyecektir ve bu hususun değerlendirmelere eklenmesi gerekmektedir.

Dolaylı etkilerin en olumlu şekilde görüldüğü örnek olarak Romanowski ve Schneider'in şehirlerdeki altyapılar üzerine yapılan bir çalışmasında [26] her bir altyapı farklı segmentlere ayrılmış ve birbirleriyle olan ilişkiler tanımlanmıştır. Ayrıca önemli noktalardan birisi de altyapıların kritiklik seviyelerinin belirlenmiş olmasıdır. Bu husus ülkelerin kritik altyapılar üzerine yaptığı çalışmalar içerisinde de yer almaktadır. Bu çalışma da göze çarpan önemli bir eksiklik, olay bazlı değerlendirme yapılması olmuştur. Bu durum kritik altyapının değil olayın riskini ortaya koymayı sağlamaktadır.

Dolaylı etkilerin önemini vurgulayan Chen, Heckel-Jones, Maupin, Rubin, Bogdanor, Guo ve Haimes'a ait bir diğer çalışmada [27] GPS sistemlerindeki hataların diğer altyapıları nasıl olumsuz etkilediği gösterilmiştir. Tabii ki bu çalışma sadece bu alanla sınırlı kaldığı için kritik altyapıların geneli üzerinde yapılacak bir değerlendirme olmaktan çok uzak kalmıştır.

Avrupa komisyonu tarafından yayımlanan ve büyük bölümü varlık üzerindeki risklerin analiz ve yönetimi üzerine yoğunlaşan çalışmanın [28] katmanlı bir risk değerlendirme mimarisi sunan bölümü kritik altyapıların risk analiz ve yönetimi üzerinde yapılacak çalışmalar açısından kayda değer bir katkı sağlayacağı değerlendirilmektedir. Çünkü kritik altyapılar üzerinde yapılacak hassas değerlendirmenin derinine irdelemesinin üst katmanlara aktarımında senaryo tabanlı bir yaklaşım yeterli olmayacaktır. Aynı zamanda her bir katmanın belirlenmesi doğru senaryolar üretimini ve katmanlar arasında doğru veri akışı oluşmasını sağlayacaktır.

Varlık temelli, yapılarda genel olarak aynı olan varlıklar üzerine odaklanan, risk analiz ve yönetim çalışmalarında en temel eksikliğin tanımlamada da belirtilen genel olarak aynı olan varlıklar üzerine odaklanması olduğu değerlendirilmektedir. Çünkü genel yapılarda varlık temelinde meydana gelen riskler yerel etkileri fazla olsa bile genele büyük bir etki yaratmamaktadır. Ancak kritik altyapılarda meydana gelen riskler katmanlı ve dolaylı olarak hem altyapının kendisine hem diğer kritik altyapılara hem de topluma ciddi zararlar doğurabilmektedir. Bu nedenle yerelde kalan değerlendirmeler kritik altyapılar için doğru sonuçlar üretmeyecektir. Aşağıda, kritik altyapılarda genel varlıklar üzerine olan bazı çalışmalar irdelenmiştir.

E-devlet projesi üzerine yapılan Kumaş ve Birgören'in çalışmasında [29] ISO 27001 standardından faydalanılarak hesaplamalar yapılmıştır. Bu hesaplama yöntemi yapılacak çalışmada farklı yöntemlerle belirlenmesi gereken zafiyet ve tehdit olasılıkları, dolaylı etkiler, önem düzeyleri gibi ifadelerin belirlenmesi açısından hem kolaylık sağlayacağı hem de yeknesaklık oluşturacağı değerlendirilmektedir. Bu çalışmada karşı önlemlerin sadece maliyet odaklı belirlenmesi ve hesaplamaların

tehdit olasılıkları üzerinden yürütülmesi tek parametreye bağlı yöntemlerin doğru sonuçlar üretemeyeceği gerçeğini göstermektedir.

Kritik altyapıların korunmasına yönelik Feglar ve Levy'e ait çalışmada [30] benzer şekilde ISO/IEC 17799 standardına göre hesaplamalar yürütülmüştür. Değer belirleme işlemi neticesinde de üretilen değerler kabul görmüş bir analiz yöntemiyle hesaplamaya tabi tutulmuştur. Burada da görülen ciddi ve benzer bir sorunda hesaplamalar sadece önemli olduğu değerlendirilen varlıklar üzerinden yürütülmüştür. Kritik altyapıların katmanlı ve dolaylı etkilerinin nereye varabileceği kestirilemeyeceği için hiçbir bileşenin göz ardı edilmemesi gerekmektedir.

Heo, Shin, Lee ve Won'un çalışması [31] üzerinde yapılan incelemede ITU-T X.805 koruma modeli üzerine oturan bir yaklaşım yürütüldüğü görülmektedir. Sierla, Hurkala ve Charitoudi'e ait başka bir çalışmada da [32] elektrik dağıtım sistemlerinin IEC 61499 ve IEC 61850 standartlarına uyumluluğu aranmıştır. Bu çalışmalar bize değerlendirmeler yapılırken belli standartlar üzerinden hesaplamaların yürütülmesinin önemli faydalar sağladığını göstermiştir. Bununla birlikte tüm bu çalışmalarda yapılan en büyük hatanın ise belli noktalar üzerinde odaklı kalarak bütünün görülememesi olduğu değerlendirilmektedir.

Yapılan çalışmaların bazılarında [33][34] makine öğrenmesi, yapay sinir ağları, uzman sistemler gibi yapay zekâ yöntemlerinden de faydalanıldığı görülmüş ancak bu yöntemlerin genel olarak hesaplamaları hızlandırma amacına yöneldiği tespit edilmiştir. Risk analiz ve yönetim modelinin ortaya konmasını müteakip hesaplamalara fayda sağlayacağı değerlendirilmekle birlikte modelin tasarımı üzerinde kullanılabilir olmadığı kıymetlendirilmiştir.

3. Kritik Altyapılarda Risk Analizi ve Yönetimi Çerçeve Altyapısı

Bu çalışmanın amacı genel risk analiz ve yönetim süreci yaklaşımlarını ve uluslararası standartları bütüncül olarak değerlendirerek kritik altyapılar için modüler bir risk analiz ve yönetim çerçevesi sunmaktır. Çerçevenin genel yapısını oluştururken ISO 31000 Risk Yönetim Süreci modelindeki yaklaşım, özellikle toplam kalite yönetimi süreçlerinde önemli bir yer tutan PUKÖ çevrimine uyumluluğu göz önünde bulundurularak, temel alınmıştır. Çerçevenin her adımında bahse konu çevrim kriterlerine uyum sağlamaya özen gösterilmiştir.

Katmanlı mimari, senaryo tabanlı yaklaşım, varlık-açıklık-tehdit-karşı önlem modeli, uluslararası standartlara uyumluluk, perspektif değerlendirme ve literatürde konu üzerine yapılmış olan çalışmalardan elde edilen çıkarımlarla tasarlanan modelin temel taşları oluşturulmuştur.

Bilişim sistemlerinde kullanılan genel varlıklar temel alınarak işlem yapılacak varlık katmanı, kritik altyapıların hedeflerinin, bu hedefleri gerçekleştirmede kullanılacak varlıklarla ilişkilendirilerek değerlendirmeye tabi tutulduğu sistem katmanı ve nihayetinde kritik altyapının genelinin irdelenmesi ve diğer altyapılarla etkileşim hesaplamalarının yapılacağı toplum katmanından oluşacak Şekil–3'te gösterilen 3 aşamalı bir katmanlı mimari tasarımı öngörülmüştür.

Varlık katmanındaki analiz genel bilişim sistemleri üzerinde kabul görmüş değerler ile sisteme uygulanan yöntemlerin etkilerini birleştiren bir fonksiyon ile hesaplanmakta olup kullanılacak değişkenler için ise NIST Kritik Altyapılar Koruma Çerçevesi ve ISO 27005 standardı referans alınmıştır.

Sistem katmanında perspektif bir bakış açısıyla üretilecek senaryo tabanlı model değişken ve değerleri, varlık katmanının risk puanları ile sistem içerisindeki personelle karşılıklı etkileşim vasıtasıyla üretilecektir. Toplum katmanında, sistem katmanından alınan veriler ile mevcut altyapı ve diğer altyapıların etkilenme değerlerini parametre olarak alan fonksiyon kullanılarak sonuç değer üretilecektir.

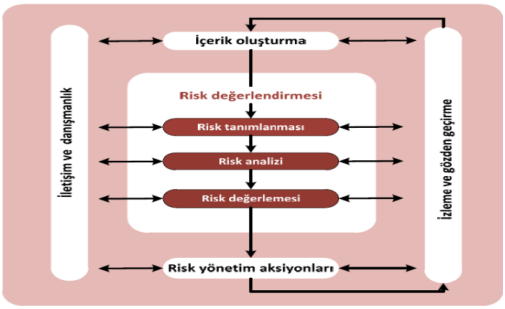
Şekil – 3: Kritik Altyapılarda Risk Analizi ve Yönetimi Çerçevesi Modeli

3.1 Kritik Altyapılarda Risk Analizi ve Yönetimi Çerçevesi

Toplam kalite yönetimindeki PUKÖ döngüsünün temelinde ISO 31000 Risk Yönetim Süreci yaklaşımının Şekil–4'te yer alan tasarımı üzerine kurulacak çerçeve 5 adımdan oluşmaktadır. Bu adımlar içerisinde gerçekleştirilmesine dikkat

edilecek bir diğer önemli husus ise risk yönetim sürecinin 7R ve 4T'si olarak ifade edilen aşağıdaki aşamalardır.

- "Recognition" – Riskin tanımlanması veya tanınması
- "Ranking" – Riskin sıralanması ya da değerlemesi
- "Responding" – Belirgin risklere cevap verme
  - ❖ 'Tolerate' – Tolere etme
  - ❖ 'Treat' – Müdahale etme
  - ❖ 'Transfer' – Transfer etme
  - ❖ 'Terminate' – Sonlandırma
- "Resourcing" – Kontrollere kaynak ayrılması
- "Reaction" – Reaksiyon planı yapılması
- "Reporting" – Risk performansının raporlanması ve takibi
- "Reviewing" – Risk yönetim çerçevesinin gözden geçirilmesi



Şekil – 4: Kritik Altyapılarda Risk Analizi ve Yönetimi Çerçevesi Modeli Adımları

a. İçerik Oluşturma

PUKÖ döngüsünün planlama aşamasını oluşturmakta ve risk yönetim sürecinin mimari, strateji ve protokollerinin üretileceği evreyi teşkil etmektedir.

Risk mimarisi oluşturulurken altyapının hem idari ve teknik organizasyonu hem de risk yönetim organizasyonu, iletişim, yetki, raporlama vb. mekanizmaları belirlenir. Perspektif değerlendirme gerektiren aşamaların belirlenmesinde ve sistemdeki risklerin yönetiminde önemli rolleri olması nedeniyle etkili bir organizasyon yapısı oluşturulması ve yetkin personel görevlendirmesi risk yönetimi açısından büyük önem arz etmektedir.

Risk protokolleri ve strateji belirleme aşamasında NIST tarafından yayımlanan kritik altyapılarda siber güvenliğin artırılmasına yönelik çerçeveden [35] faydalanılmasının sistemin karakteristiğini çıkarmada ortaya çıkacak karmaşık ve zorlu süreci ortadan kaldıracağı ve kabul görmüş bir yaklaşım ile standart bir süreç oluşturulacağı değerlendirilmektedir.

NIST tarafından belirlenen çerçeve 3 bölümden oluşmakta ve ilk bölümde sistem gerekliliklerini belirten bir çekirdek sınırları çizilmektedir. Şekil-5'de genel şablonu yer alan çekirdeğe risk değerlendirmesi aşamasında kullanılmak üzere varlık ve zafiyet sütunu eklenerek sistem verileri aktarılabilecektir.

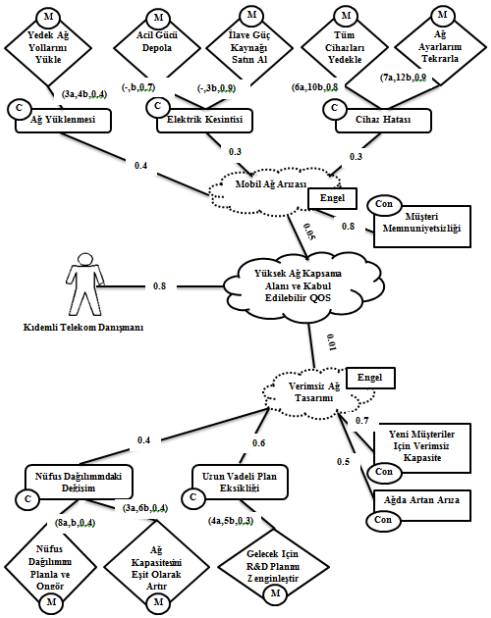
Fonksiyonlar	Kategoriler	Alt Kategoriler	Bilgilendirici Referanslar
TANIMLAMA			
KORUMA			
TESPİT			
KARŞILIK VERME			
KURTARMA			

Şekil – 5: Sistem Gereklilikleri Şablonu [35]

Katmanlı mimari tasarımında her bir katman içerisinde ayrı risk değerlendirmesi yapılacak ve sonuçlar bir sonraki aşamanın girdileri olacaktır. Yukarıda belirtilen değerlendirme ile varlık katmanının girdileri üretilecek risk değerlendirmesini müteakip üretilecek veriler sistem katmanına aktarılacaktır. Sistem katmanında değerlendirmenin yapılabilmesi amacıyla risk yönetim organizasyonu tarafından perspektif yaklaşımla senaryolar üretilmesi gerekmektedir. Senaryo tabanlı yaklaşım için örnek bir yapı Şekil–6'da olduğu gibidir. Burada sistemin teknik ve idari açıdan yönetim organizasyonunun da rolü risk değerlendirmesine dâhil edilmiştir.

Risk değerlerinin hesaplanma yönteminin belirlenmesi, her bir katmanda belirlenmesine/ üretilmesine ihtiyaç duyulan verilerin ortaya konması adına ilk adım olacaktır. Bu veriler belirlenirken 2 farklı yol üzerinden ilerlenmesi ve hem yapı üzerindeki en yüksek riskin hem de ortalama riskin ortaya konması daha esnek bir değerlendirme imkânı sunacaktır. Risk yönetim standartlarında [22][23][24] risk hesabı irdelenirken karşımıza ifade farklılıkları olmakla birlikte temelde odaklanılan 2 önemli parametre çıkmaktadır: etki/büyüklük/şiddet vb. ve olasılık/oran vb. Burada yapılacak hesaplamalarda temel alınacak bu fonksiyon parametrelerine ek olarak literatürde teorik olarak etkilerinin önemi birçok çalışmada vurgulanan dolaylı etki puanları eklenecektir. Dolaylı etki puanı hesabında da genel risk puanı hesabında kullanılan parametreler temel

alınacaktır. Bu kapsamda her bir katman özelindeki hesaplama yöntemleri adımlar halinde aşağıda verilmektedir.



Şekil – 6: Senaryo Tabanlı Yaklaşım Modeli [25]

a. Varlık katmanında risk puanının hesaplanmasında kullanılacak ve temel alacağımız risk puanı hesaplama fonksiyonunu karşılayan 2 parametre ön plana çıkmaktadır: Varlık değeri ve riskin gerçekleşme olasılığı. Normalize puanı tüm katmanlardaki hesaplamada kullanılarak üretilen verilerin belirli bir aralığa indirgenerek ifade edilmesini sağlayacaktır. Bu bilgiler ışığında (1) ve (2) sayılı eşitliklerle varlık üzerindeki risk hesaplanmaktadır.

$$R_{vO} = V_{DO} * P_O * N_{PS} \quad (1)$$

$$R_{vM} = V_{DM} * P_M * N_{PS} \quad (2)$$

Sembol	Tanım
R_{VO}	Varlık Üzerindeki Risk (Ortalama)
R_{VM}	Varlık Üzerindeki Risk (En Yüksek)
V_{DO}	Varlık Değeri (Ortalama)
V_{DM}	Varlık Değeri (En Yüksek)
P_O	Olasılık (Ortalama)
P_M	Olasılık (En Yüksek)
N_p	Normalize Puanı
N_{PS}	Standart Normalize Puanı, 0,01 olarak kullanılacaktır.

Burada varlık değerinin belirlenmesine etki eden 3 önemli faktör bulunmaktadır. Bunlar varlığın bilgi güvenliği açısından önem düzeyi, varlığın mali değeri ve varlığın etkisiz kalması/zarar görmesi durumunda diğer varlıkları etkileme puanı yani dolaylı etkiler olarak görülmektedir. Bilgi güvenliği önem düzeyi ve mali değer risk yönetim standartlarında [22][23][24] varlık değeri irdelemesinde odaklanılan en önemli 2 parametre olmaktadır. Risk puanı hesabında kullanılmasına karar verilen fonksiyonun etki/büyüklük/şiddet vb. parametresinde alt parametre olarak sisteme dâhil edilmeye karar verilen dolaylı etki puanı burada fonksiyona eklenmiştir.

Varlığın bilgi güvenliği açısından önem düzeyi [10] Çizelge–1'de yer alan değerler üzerinden organizasyon tarafından belirlenebilir. Tablonun sütun değerleri artırılarak daha hassas bir hesaplamada gerçekleştirilebilir. Tabii ki bu değerlendirmeyi yapacak organizasyonun risk yönetim birimi olacaktır. Bilgi güvenliği düzeyinin en üst seviyesinin belirlenmesi risk oranını en doğru şekilde ortaya koyacağı değerlendirilmekte olup bu değerin ortaya konması için tüm parametrelerin birbirinin değerlerini katlayarak artıracağı görüşü daha fazla ön plana çıkmıştır. Bilgi güvenliği değerlerinin belirlenmesine yönelik standart yöntemler oluşturulmasına yönelik çalışmalar [36] bulunmaktadır. Kabul görmüş bir çalışmanın çerçeve içerisine dâhili ile perspektif yaklaşımdan standartlaşmaya daha da yaklaşılabilecektir.

Çizelge – 1: Bilgi Güvenliği Değerlendirme Matrisi

	Gizlilik(G)	Bütünlük(B)	Erişilebilirlik(E)
Düşük			
Orta		✓	
Yüksek	✓		✓
Bilgi Güvenliği Puanı	3	2	3

Varlık değerinin bir diğer unsuru mali değer olacaktır. Bu husus sadece varlık değeri ile kalmayıp genel risk değerlendirmesine de etki etmekte ve özellikle mali açıdan daha ayrıntılı risk analiz/değerlendirme çalışmaları [37][38] da yapılmaktadır. Varlığın mali değerinin hesabında, elde etme maliyeti, işlem maliyeti ve kaybedilen iş fırsatı gibi üç öğe öne çıkmaktadır [38]. Elde etme maliyeti varlığın sisteme kazandırılması amacıyla harcanan mali değeri, işlem maliyeti varlığın idame ettirilmesi amacıyla gerekli olan mali değeri, kaybedilen iş fırsatı ise varlığın

zarara uğraması/devre dışı kalması durumunda ortaya çıkacak mali kaybı ifade etmekte olup (3) sayılı eşitlikte gösterildiği gibi toplam maliyetin temelini oluşturmaktadır.

$$F_v = \sum_{i=1}^{n} DY_i L_i + \sum_{j=1}^{m} C_j M_j + IA \quad (3)$$

Sembol	Tanım
F_V	Varlığın mali değeri
DY	Varlık için kullanılan donanım ve yazılım sayısı
L	Varlıkta kullanılan donanım ve yazılımın ücreti
C	Varlığın idamesi için çalışan personel sayısı
M	Personel ücretleri
I	Kaybedilen iş fırsatı
A	Servis dışı kalma süresi

Varlık değerine etki edecek son faktör varlığın zarara uğraması/devre dışı kalması durumunda etkilenecek diğer sistemlerin etkilenme düzeyi olup (4) ve (5) sayılı ifadelerde belirtildiği şekilde etkilenen varlığın önem düzeyi ve etkilenme oranıyla ifade edilebilir.

$$D_{vO} = \sum_{i=1}^{n} V_{\ddot{o}i} O_{vi} * N_{PS} \,/\, n \quad (4)$$

$$D_{vM} = Max(V_{\ddot{o}} * O_v) * N_{PS} \quad (5)$$

Varlık değerinin belirlenmesi amacıyla yukarıda belirtilen eşitliklerin parametreleri içerik oluşturma safhasında üretilmesini müteakip (6), (7) ve (8) sayılı eşitlikler ile varlık değerinin hesaplaması yapılabilecektir.

$$N_{PV} = Max\big(MP(G,B,E)\big) * F_K * Max(D_v) \quad (6)$$

$$V_{DM} = MP(G,B,E) * F_v * D_{vM}/N_{PV} * N_{PS} \quad (7)$$

$$V_{DO} = MP(G,B,E) * F_v * D_{vO}/N_{PV} * N_{PS} \quad (8)$$

Sembol	Tanım
N_{PV}	Varlık Değerinin Normalize Puanı
F_K	Kritik Altyapının Mali Değeri
D_{VO}	Varlık Üzerindeki Dolaylı Etki (Ortalama)
D_{VM}	Varlık Üzerindeki Dolaylı Etki (En Yüksek)
$V_{\ddot{O}}$	Etkilenen varlık önem düzeyi
O_V	Etkilenen varlığın etkilenme oranı
MP(G,B,E)	En Üst Düzey Bilgi Güvenliği Değeri

Riski gerçekleşme olasılığını değerlendirecek olursak; varlık üzerinden risk gerçekleşme ihtimaline etki eden risk yönetim standartlarında [22][23][24] en önemli 2 faktör, varlık üzerindeki zafiyetler ve bu zafiyetler karşısında varlık üzerinde risk oluşturan tehditler olarak karşımıza çıkmaktadır. Bu çerçevede risk gerçekleşme olasılığının üretim fonksiyonun parametrelerinin zafiyet ve tehdit olduğu görülmektedir.

$$P_M = Max(Z * T) * N_{PS} \quad (9)$$

$$P_O = \frac{\sum_{i=1}^{n} Z*T}{n} * N_{PS} \quad (10)$$

Sembol	Tanım
Z	Zafiyet
T	Tehdit

Zafiyet ve Tehdit değerleri yukarıda belirtilen çerçeve ile organizasyon tarafından belirlenerek (9) ve (10) sayılı eşitlikler üzerindeki yerlerini alacaklardır.

b. Sistem katmanında (11) ve (12) sayılı eşitliklerde belirtilen riskin hesaplanması senaryo tabanlı yaklaşım gereği kurulacak senaryoların hedefleri üzerinden yapılacaktır. Hedeflerin gerçekleşmemesi riski 3 temel faktöre dayanmaktadır. En önemli parametre (13) ve (14) sayılı eşitlikle gösterilen hedeflerin gerçekleşmesine etki eden varlıklar üzerindeki risk puanlarıdır. Bahse konu varlıkların hedef üzerindeki etki oranları bir diğer faktör olarak karşımıza çıkmaktadır. Dolaylı etkiler tüm risk değerlendirmelerinde olduğu gibi bu analizde de karşımıza çıkacak olup dolaylı etki olarak varlık katmanından farklı olarak insan faktörü işleyiş içerisine dâhil edilmesi gerekmektedir. Çünkü sistem sorumluları sistemin hedeflerine ulaşması açısından önemli bir rol almaktadır. Dolaylı etki puanına bir diğer etki eden husus hedefleri sistem içerisinde yer alan diğer hedefleri etkileme değeridir.

$$R_{sO} = R_{PO} * D_{sO} * N_{PS} \quad (11)$$

$$R_{sM} = R_{PM} * D_{sM} * N_{PS} \quad (12)$$

$$R_{PO} = \Big(\frac{\sum_{i=1}^{n}\Big(\frac{\sum_{j=1}^{m} R_{vOj}{}^{*}O_{RTi}}{m}\Big)}{n} + \frac{\sum_{k=1}^{o}\Big(\frac{\sum_{l=1}^{p} R_{vOl}{}^{*}O_{REk}}{p}\Big)}{o} + \frac{\sum_{t=1}^{r}\Big(\frac{\sum_{u=1}^{s} R_{vOu}{}^{*}O_{RGt}}{s}\Big)}{r}\Big)N_{PS}/3 \quad (13)$$

$$R_{PM} = Max(O_{RT}, O_{RE}, O_{RG}) * R_{vM} * N_{PS} \quad (14)$$

Sembol	Tanım
R_{SO}	Sistem Üzerindeki Risk (Ortalama)
R_{SM}	Sistem Üzerindeki Risk (En Yüksek)
R_{PO}	Risk Puanı (Ortalama)
R_{PM}	Risk Puanı (En Yüksek)
D_{SO}	Sistem Üzerindeki Dolaylı Etki (Ortalama)
D_{SM}	Sistem Üzerindeki Dolaylı Etki (En Yüksek)
O_{RT}	Tehlike Risk Oranı
O_{RE}	Engel Risk Oranı
O_{RG}	Gereklilik Risk Oranı

Risk oranı literatürdeki yöntemsel yöntemler kullanılarak organizasyonun yönetimi tarafından belirlenmelidir. Eşitlik (15) ve (16)'da yer alan dolaylı etki puanı içerisinde yer alacak insan faktörü, etkilenen diğer hedeflerin önem düzeyi ve etkilenme

oranları da organizasyon tarafından belirlenmesi gerekmektedir. Ortaya çıkacak değerler ile aşağıdaki eşitlikler kullanılarak dolaylı etki puanı da elde edilmiş olacaktır.

$$D_{sO} = (\sum_{i=1}^{n} C_{Hi} \sum_{j=1}^{m} H_{\ddot{o}j} O_{Hj}) * N_{PS}^2/nm \quad (15)$$

$$D_{sM} = Max(C_H H_{\ddot{o}} O_H) * N_{PS}^2 \quad (16)$$

Sembol	Tanım
$H_{\ddot{O}}$	Etkilenen hedefin önem düzeyi
O_H	Hedefin etkilenme oranı
C_H	Hedefin gerçekleşmesinde görevli organizasyon personelinin yetkinlik düzeyi

c. Toplum katmanında kritik altyapı üzerindeki genel risk değerlendirmesi (17) ve (18) sayılı ifadeler ile üretilmiş olacaktır. Toplum katmanındaki risk düzeyini etkileyen temel değer hedeflerin stabilizesi yani gerçekleşme oranı ve bahse konu hedeflerin her birinin kritik altyapı için önem düzeyi olduğu görülmektedir. Buradaki yapıya etki edecek (19) ve (20) sayılı eşitlikle hesaplaması gösterilen dolaylı etki puanı için 2 önemli parametre göze çarpmaktadır. Bunlar kritik altyapının etkisiz kalması/zarar görmesi durumunda etki altında kalacak diğer altyapılar ve kurulan sisteme büyük etkisi olan Bilgi Güvenliği Yönetim Sisteminin tutarlılık seviyesidir.

$$R_{tO} = \frac{\sum_{i=1}^{n} H_{Si} H_{\ddot{o}i}}{n} * D_{tO} * N_{PS}^2 \quad (17)$$

$$R_{tM} = Max(H_S H_{\ddot{o}}) * D_{tM} * N_{PS}^2 \quad (18)$$

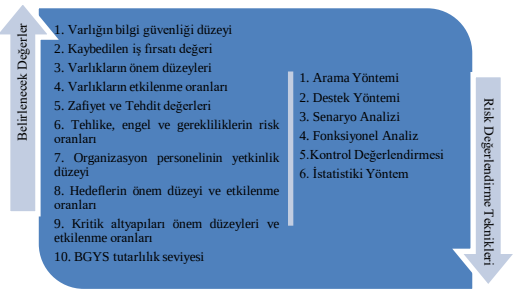
$$D_{tO} = \frac{\sum_{i=1}^{n} K_{\ddot{o}i} O_{Ki}}{n} * BGYS * N_{PS}^2 \quad (19)$$

$$D_{tM} = Max(K_{\ddot{o}} O_K) * BGYS * N_{PS}^2 \quad (20)$$

Sembol	Tanım
R_{tO}	Kritik Altyapı Üzerindeki Risk (Ortalama)
R_{tM}	Kritik Altyapı Üzerindeki Risk (En Yüksek)
D_{tO}	Kritik Altyapı Üzerindeki Dolaylı Etki (Ortalama)
D_{tM}	Kritik Altyapı Üzerindeki Dolaylı Etki (En Yüksek)
H_S	Hedef stabilizesi/gerçekleme değeri
$H_{\ddot{O}}$	Hedefin önem düzeyi
$K_{\ddot{O}}$	Etkilenen diğer kritik altyapıların önem düzeyi
O_K	Etkilenen diğer kritik altyapıların etkilenme oranı
BGYS	Bilgi Güvenliği Yönetim Sisteminin tutarlılık seviyesi

Yukarıda belirtilen fonksiyonlardaki ifadeler içerisinde önemli bir yer tutan bazı değerler risk yönetim organizasyonu tarafından belirlenecek değerlerdir. Tabii ki burada organizasyonun söz konusu değerleri nasıl belirleyeceği sorusu karşımıza çıkmaktadır.

Tasarlanan çerçevenin genelinde olduğu üzere buradaki yaklaşımda benzer şekilde uluslararası kabul görmüş standart/doküman vb. üzerinden yürütülmesi şeklinde olacaktır. ISO tarafından belirlenmiş 31010 Risk Yönetimi ve Risk Değerlendirme Teknikleri Standardı önümüze eldeki verilerden anlamlı sonuçlar üretebilmemiz amacıyla birçok yöntem sunmaktadır. Risk Yönetim Organizasyonu eldeki veriler, tekniklerin kabul görmüşlük seviyeleri, sonuç üretimiyle tekniğin uyumluluğu vb. parametreleri değerlendirerek tekniği belirlemeli ve bahse konu tekniği kullanarak istenen verinin üretimini sağlamalıdır. Varlık değerinin belirlenmesi aşamasında kullanılan mali değerin parametrelerinden olan donanım ve yazılım lisans bedeli, personel maaşları gibi sabit değerler bu değerlendirme kapsamında olmayacak, değerlendirme sadece göreceli kavramlar üzerinde yapılacaktır. Şekil–7'de belirlenmesi gereken veriler ile kullanılabilecek teknikler gösterilmiştir.



Şekil – 7: Belirlenecek Değerler ve Risk Değerlendirme Teknikleri

İçerik oluşturma safhasında risk yönetim organizasyonu tarafından belirlenmesine ihtiyaç duyulan değerler Çizelge–2'de çerçeveyi daha net görebilmek adına birleştirilmiştir (Risk mimari, protokol ve stratejileri hariç). Risk Yönetim Sürecinde risk mimarisi olarak; roller ve sorumluluk ile raporlama yapısı, risk stratejisi olarak; risk yönetim felsefesi/politikası, risk protokolleri olarak; kurum içi prosedür/kurallar ile yönetim yöntemleri, araçlar ve teknikler belirlenmelidir. Bununla birlikte bu aşama ile risk yönetim sürecinin risk tanımlama ve risk değerleme maddeleri gerçekleştirilmiş olmaktadır.

Çizelge – 2: Belirlenecek Değerler

KATMAN	BELİRLENECEK DEĞERLER
Varlık Katmanı	• Sistem gerekliliklerinin belirlendiği NIST çerçevesine varlık – zafiyet değerinin eklenmesi ve zafiyet puanlarının ortaya konması • ISO 27005 de yer alan tehditlerin gerçekleşme olasılıklarının açık kaynaklardaki ve sistem geçmişindeki veriler kullanılarak belirlenmesi • Varlıkların mali değerlerinin hesaplanması amacıyla bu değer içerisinde kaybedilen iş fırsatı değerinin belirlenmesi • Her bir zafiyet – tehdit eşleşmesindeki karşı önlemlerin belirlenmesi • Varlıkların sistemin diğer varlıklarını etkileme durumu göz önüne alınarak dolaylı etki değerlerinin belirlenmesi • Varlıkların bilgi güvenliğinin 3 önemli unsuru olan Gizlilik, Bütünlük, Erişilebilirlik açısından değerinin belirlenmesi • Varlıkların önem düzeyleri ve diğer varlıklarından etkilenme oranlarının belirlenmesi
Sistem Katmanı	• Kritik altyapının hedefleri göz önüne alınarak senaryoların üretilmesi • Senaryolarda hem organizasyon hem de tehlike, engel, gereklilik vb. girdilerin etki oranlarının belirlenmesi • Organizasyonda görevli personelin nitelik değerlerinin belirlenmesi • Senaryolarda sonucunda ortaya çıkacak sonuçların ve hafifletme yöntemlerinin belirlenmesi • Hedeflerin önem değerleri ve diğer hedeflerden etkilenme puanlarının belirlenmesi
Toplum Katmanı	• Kurulan risk organizasyonunun etkinlik seviyesinin belirlenmesi • Diğer kritik altyapılara etki oranları ve önem düzeylerinin belirlenmesi

b. Risk Değerlendirmesi

Risk değerlendirme süreci; risk belirleme, analiz ve kıyaslama olmak üzere 3 aşamadan oluşmaktadır. Risk belirleme aşaması uluslararası standartların şablonları kullanılması ve içerik oluşturma aşamasındaki senaryo üretimi sayesinde büyük oranda tamamlanmıştır. Analiz aşaması her bir katman için ayrı risk analiz süreci yürütüldüğü için ayrı değerlendirilmesi gerekecektir.

Tasarlanan çerçevenin temeli literatürdeki en kabul görmüş yöntem olan varlık – açıklık – tehdit modeli üzerine oturtulmuştur. Bu kapsamda varlık katmanındaki risk analizinde risk değerinin belirlenmesi için bahse konu modelde en yaygın olarak kullanılan, Risk = Varlık Değeri * Olasılık eşitliğinin tercih edilmesinin uygun olacağı değerlendirilmiştir. Varlık değeri belirlenirken literatürde en temel olarak kullanılan yaklaşımlar; bilgi güvenliği kriterleri, mali değer ve sistemin diğer bölümlerine etkisidir. Her bir yaklaşım tasarlanan modellerde ayrı olarak değerlendirilse de varlık değeri için ayrım yapılamayacağı düşünülmüştür ve içerik katmanında ayrıntılı belirtilen hesaplama ortaya çıkmıştır. Varlık üzerindeki riski etkileyen en önemli değerler zafiyetler ve bu zafiyetleri kullanan tehditlerdir, bu nedenle de olasılık için üretilecek formül bu iki değerin bir fonksiyonu olacaktır. Doğacak riskten etkilenecek diğer varlıklarda dikkate alınarak Risk Yönetim Organizasyonu tarafından gerekli verilerin üretilmesini müteakip sonucun alınması için sadece formüllerde değerlerin yerine konması kalacak ve varlıklar üzerindeki risk değerleri ortaya çıkacaktır.

Sistem katmanında risk hedefe olan etki değeri ile bunun olasılığı, sistem sorumluların yetkinlik seviyesi ve etkilenen diğer hedeflerin bir fonksiyonu olacak şekilde değerlendirilmiştir. Buradaki en önemli parametre hedefin risk değeri ve değeri de belirleyen varlık katmanındaki hedefi etkileyen varlıkların risk puanları olmaktadır.

Sistem katmanından elde edilen veriler ve kritik altyapılar arasındaki ilişkilendirmeler ile tüm katmanlar için önemli bir yapı olan Bilgi Güvenliği Yönetim Sistemi puanının da girdi olarak eklenmesiyle toplum katmanı risk analiz tekniği tüm çerçeve için risk analiz sonucunu üretecektir.

Risk değerlendirmesinin son aşaması olan kıyaslama işlemi içerik oluşturma bölümünde belirlenen ve NIST siber güvenlik çerçevesine dayanan risk stratejisine göre değişkenlik gösterebilecektir. Tasarlanan çerçevenin sonucuna göre kıyaslamalar üretilebileceği gibi ara katmanlarda da kıyaslamalar üretilebilecektir.

c. Risk Yönlendirme

Risk değerlendirme aşamasını müteakip tasarlanan çerçeve, sistemin sorunlu alanlarını ortaya koymuş olacaktır. Bu aşamada ise risk yönetim sürecinin 4T(Tolerate, Treat, Transfer, Terminate)'den hangisinin tercih edileceğine kurum kültürüne göre karar verilecektir. Kararda etkili olabilecek 3 ana unsur mevcuttur: Maliyet, Zaman, Etkinlik. Bahse konu değerler kullanılarak oluşturulan (21) sayılı

eşitlik ile bir eşik puanı üretilerek risk yönlendirme işleminin yöneleceği süreç belirlenebilecektir.

$$E = (V_{DM} - (F_{KÖ} + IA)) * O_R \quad (21)$$

Sembol	Tanım
E	Risk yönlendirmede kullanılacak eşik değeri
$F_{KÖ}$	Karşı önlem maliyeti
O_R	Yapılan müdahalenin risk üzerinde yaptığı etki değeri

Eşik değeri müdahale ve transfer durumları için ayrı ayrı olarak irdelenecektir. Elde edilen veriler ışığında;

1. Eşik puanının çok düşük olduğu durumlarda mevcut riski tolere etme izlenebilecek yöntemlerden ilk akla gelen olacaktır. Tabii ki mali durum ve riski azaltma oranının yanı sıra risk organizasyonun bahse konu risk grubuna karşı oluşturduğu kültürde önemli olmaktadır.
2. Maliyet etkin çözümler yani düşük maliyet ile yüksek risk ortadan kaldırma çözümleri sisteme derhal uygulanmasında fayda gözüken durumlar olarak göze çarpmaktadır.
3. Bununla birlikte transfer çözümlerinin daha uygun maliyetli ve etkin olduğu durumlarda bu uygulamayı ön plana çıkarmakla birlikte kurum kültürü özellikle bu gibi durumlarda devreye girecek en önemli faktör olarak göze çarpmaktadır.
4. Eşik değerinin düşük olduğu durumlarda riski üreten kaynağın ortadan kaldırılması da izlenebilecek bir yöntemdir. Tabii ki burada kurumun varlık, sistem veya altyapıya olan bağımlılığı ön plana çıkacaktır.

Risk yönetim organizasyonu tarafından yapılacak irdelemeyi müteakip izlenecek yöntemler belirlenerek uygulamaya konulacaktır. Burada genel risk puanının yanı sıra katmanlar üzerinde de özel bölümlerde değerlendirmeler yapılabilecektir.

ç. İzleme ve Gözden Geçirme

Risk yönetim sürecinin sağlıklı bir şekilde işleyebilmesi adına hem PUKÖ döngüsünün hem de ISO 31000 Risk Yönetim Sürecinin önemli aşamalarından sürecin devamlı olarak izlenmesi ve sorunlu alanlar için çözüm yöntemleri üretilmesidir. Bu aşama, sisteme girdi olarak verilen verilerin değişmesi durumu ve sistemde verilerin üretiminde kullanılan mimari, strateji ve protokollerin değişmesi durumu olmak üzere iki başlık altında değerlendirilebilecektir.

Risk yönetim süreci içerisinde birçok kaynaktan çeşitli veriler sisteme girdi olarak girmektedir. Risk yönetim organizasyonu tarafından belirlenen ve her katmanda değerlendirme tabi tutulan veriler, kritik altyapıdaki hem varlık hem de insan faktörlerinin özdeğerleri (nitelik puanı, mali değeri vb.), risk değerlendirme aşaması sonucunda risk yönetim organizasyonu tarafından altyapıya uygulanmasına karar verilen karşı önlem maliyetleri ve altyapıya olan etkileri bu girdilerden en önemlileri olarak göze çarpmaktadır. Tabii ki girdi değişimleri risk analiz ve yönetim sürecinin tekrardan gözden geçirilmesini kaçınılmaz hale getirecektir.

Risk analiz ve yönetim sürecinin tekrardan gözden geçirilmesini gerektirecek bir diğer husus mimari, strateji ve protokollerin değişimidir. Birçok aşamada kullanılan risk yöntemlerinin literatürdeki gelişmelere paralel değişme ihtiyacı, yönlendirme stratejilerinin kurum kültürüne göre yeniden belirlenmesi, idari, teknik ve risk organizasyonlarının değişmesi, kurum içi kurallarda güncellemeler bahse konu değişimlerden bazılarıdır.

d. İletişim ve Danışmanlık

Kritik Altyapıların hem risk yönetim sürecinin tüm aşamalarının işlerliği açısından hem de risk analiz sürecine doğrudan etki etmesi nedeniyle etkin bir organizasyonun belirlenmesi büyük önem taşımaktadır. Organizasyon temel olarak en az üst yönetim birimi, risk yönetim birimi, denetim birimi ve iş birimlerinden oluşmalıdır. Risk yönetim birimi risk yönetim süreci ile ilgili tüm kararları verirken, denetim birimi izleme ve gözden geçirme aşamasında sürecin sağlıklı işlerliğini denetleyecektir. Ayrıca risk yönetim birimi sistemde uygulanacak protokolleri belirleyecek ve içerik oluşturma aşamasında organizasyon tarafından belirlenmesi gereken verileri sisteme girdi olarak verecektir. İş birimleri sistem yöneten birimler olması nedeniyle risk analiz sürecine doğrudan etki etmekte olup üst yönetim birimi tüm sürecin koordine ve yönetimini sağlamaktadır.

4. Vaka Çalışması ve Değerlendirme

4.1 Vaka Çalışması

Tüm dünyada olduğu gibi ülkemizde de elektrik altyapısının diğer kritik altyapılar için önem düzeyinin yüksek olması ve Türkiye'de elektrik iletim sisteminin Ankara-Gölbaşı Milli Yük Tevzi Merkezi odağında 9 farklı konumdaki dağıtım merkezlerinden yönetiliyor olmasının kritik bilgi altyapısı kavramını en iyi şekilde göstermesi nedeniyle Türkiye Elektrik İletim Sistemi Altyapısı değerlendirmemizde kullanılacak en uygun örnek olacağı kıymetlendirilmiştir. Bununla birlikte Türkiye'deki

elektrik üretim sistemlerinin doğu bölgelerinde elektrik kullanım oranının batı bölgelerinde yoğunlaşması da bahse konu sistemin önemini bir kat daha artırmaktadır.

a. İçerik Oluşturma

1. **Risk Mimarisi**: Analiz edilen organizasyondaki mimari yapı en az yönetim birimi, risk yönetim komitesi, denetim komitesi ve iş birimlerinden oluşmalıdır. Elektrik İletim Şirketi özelinde bir yapı kurulacağı gibi Enerji ve Tabii Kaynaklar Bakanlığı genelinde bir organizasyonda kurulabilecektir. Mimarı yapı hem tüm risk analiz ve yönetim sürecinin belirleyen birimlerin oluşturulması açısından hem de bu birimlerin olması gerekene yakınlığı ile risk analiz ve yönetim sürecine etkisi açısından önemlidir. Mimari yapı yinelemeli olarak çalışmaktadır.
2. **Risk Stratejisi**: Temel olarak risk değerlendirme aşaması sonunda belirlenen risk puanlarının kabul edilebilirlik seviyelerine göre hangi yönlendirmelerin yapılacağının belirlendiği bu aşamada strateji olarak aşağıdaki kriterler uygulanacaktır.
    a. Örnek üzerindeki değerlendirmede genel risk puanının %1,5 ve üzeri değeri kabul edilebilir olarak görülmeyecek,
    b. Bununla birlikte ağ altyapısı üzerinde de varlık bazlı risk puanı olarak %10 ve altı değerler aranacak,
    c. Veri tabanları üzerinde herhangi bir risk transferi işlemi uygulanmayacak,
    d. Risk sonlandırma amacıyla yapılacak işlemlerde bilgi güvenliği değeri 9 olan varlıklar sistemden çıkarılmayacaktır.
3. **Risk Protokolleri**: Belirlenecek risk yönetim organizasyonunun en önemli görevlerinden birisi değerleme aşamasında organizasyon tarafından belirlenmesi gereken verilerin üretim yöntemlerinin belirlenmesidir. Burada uluslararası standartlar üzerinden yöntem belirlemesi yapılacağı gibi geçmiş veriler ve hâlihazırda literatürdeki standart puanlar üzerinden bir değerleme de yapılabilecektir. Bu kapsamda belirlenecek değerler için örneğimizde uygulayacağımız protokoller Şekil–8'de olduğu gibidir. Birden fazla belirlenen protokolün değerlerinin aritmetik ortalaması hesaplanacaktır.

Şekil – 8: Risk Protokolleri

4. **Değerleme**: Belirlenen risk protokolleri çerçevesinde risk organizasyonu tarafından belirlenecek değerler risk değerlendirme aşamasına aktarılacaktır. Bununla birlikte belirlenmesi gereken bir diğer husus ise veriler arasındaki ilişkilerin ortaya konmasıdır. Bu kapsamda değerleme işleminde ilk adım olarak uluslararası standartlarda olması gereken yapıyla kıyaslama yapılarak varlıklardaki zafiyetlerin ortaya çıkarılması işlemidir. NIST tarafından belirlenen çerçeveye varlık ve zafiyet sütunu eklenmiş bu sayede varlıkların üzerindeki zafiyetlerin oranları daha net görülebilecek bir seviye kazandırılmıştır.

Varlıklarda bulunan zafiyetlerin tespitini ve tablo üzerinden yapılacak analiz ile risk değerlendirme aşamasında puanlamalarının yapılmasını müteakip bahse konu zafiyetlerle tehditlerin ilişkilendirilmesi ve varlıklar üzerindeki risklerin ortaya konması işlemi gerçekleştirilecektir. Bu kapsamda gerekli tablo üretilerek varlıklar üzerindeki tüm riskler görülebilir hale getirilecektir.

Varlık katmanında verilerin üretilmesinden sonra bahse konu verilerin sistem katmanına aktarımı ve sistem katmanında kullanımına yönelik oluşturulacak veri seti uygun şekilde üretilecektir. Veri seti bir elektrik santrali temel alınarak örneklendirilecektir. Burada kurulacak ilişkilendirme ile değerlendirme aşamasında sistem katmanının risk hesaplamalarına ışık tutulacaktır.

Sistem katmanındaki senaryoların oluşturulmasından sonra hazırlanması gereken son tablo senaryo hedeflerinden etkilenen diğer kritik altyapı/sistemler tasarlanan çerçeveye eklenerek değerleme işlemi

tamamlanacaktır. Tüm kritik altyapı üzerindeki nihai risk değerlendirme işlemi bu aşamada gerçekleştirilecek ilişkilendirmeler ve diğer katmanlardan gelecek veriler ışığında hesaplanabilecektir.

b. Risk Değerlendirmesi

Bu aşamada risk organizasyonu tarafından belirlenen veriler ve değerleme aşamasında ortaya konan ilişkiler kullanılarak ortaya konan eşitlikler üzerinden risk puanı hesaplamaları gerçekleştirilir. Risk organizasyonu tarafından belirlenen protokoller üzerinden verilerin belirlendiği varsayılarak hesaplama işlemine geçilecek olursa;

1) **Varlık Katmanı**: Ağ altyapısı, veri tabanları ve disk üniteleri için örnekleme olarak risk puan hesaplamaları yapılacaktır. Varlık değeri hesaplaması ile işe başlanacak olursa ilk olarak normalize puanının hesaplanması gerekecektir. (FAğ Altyapısı= 40, FVeri tabanları= 38, FDisk Ünitesi= 35 olarak alınacaktır.)

$$N_{PV} = Max\big(MP(G,B,E)\big) * F_K * Max(D_v)$$

$$N_{PV} = 9 * 100 * 90 = 81000$$

Varlıkların mali değerleri hesaplanmış olarak kabul edilerek dolaylı etki puanları hesaplanacak ve bu değerlerle varlık değerleri bulunacaktır.

$$D_{vO} = \sum_{i=1}^{n} V_{öi} O_{vi} * N_{PS} \,/\, n$$

$$D_{vO} = \big((90 * 70) + (95 * 80) + \cdots..\big) * 0{,}01/n = 80\ (Ağ\ Altyapısı)$$

$$D_{vO} = \big((80 * 75) + (90 * 60) + \cdots..\big) * 0{,}01/n = 70\ (Veri\ Tabanları)$$

$$D_{vO} = \big((85 * 70) + (90 * 75) + \cdots..\big) * 0{,}01/n = 75\ (Disk\ Üniteleri)$$

$$V_{DO} = MP(G,B,E) * F_v * \ D_{vO}/N_{PV} * N_{PS}$$

$$V_{DO} = 8 * 40 * \ 80/81000 * 0{,}01 = 31{,}6(Ağ\ Altyapısı)$$

$$V_{DO} = 8 * 38 * \ 70/81000 * 0{,}01 = 26{,}27(Veri\ Tabanları)$$

$$V_{DO} = 9 * 35 * \ 75/81000 * 0{,}01 = 29{,}16(Disk\ Üniteleri)$$

Hesaplanan varlık değerlerinden sonra varlıkların olasılık puanları da hesaplanarak risk hesaplaması aşamasına geçilebilecektir.

$$P_O = \frac{\sum_{i=1}^{n} Z*T}{n} * N_{PS}\, P_O = \frac{(10*90)+(40*70)+\cdots..}{n} * 0{,}01 = 40(Ağ\ Altyapısı)$$

$$P_O = \frac{(30 * 70) + (15 * 85) + \cdots ...}{n} * 0{,}01 = 35(Veri\ Tabanları)$$

$$P_O = \frac{(20 * 95) + (30 * 80) + \cdots ...}{n} * 0{,}01 = 70(Disk\ Üniteleri)$$

$$R_{vO} = V_{DO} * P_O * N_{PS}$$

$$R_{vO} = 31{,}6 * 40 * 0{,}01 = 12{,}64(Ağ\ Altyapısı)$$

$$R_{vO} = 26{,}27 * 35 * 0{,}01 = 9{,}19(Veri\ Tabanları)$$

$$R_{vO} = 29{,}16 * 70 * 0{,}01 = 20{,}41(Disk\ Üniteleri)$$

2) **Sistem Katmanı**: Bu katmanda 2 hedef değeri örnek hesaplamaya tutulacak ve elde edilen sonuçlar bir üst katmana aktarılacaktır. Örnek olarak "Beslenen Noktalara Kesintisiz Elektrik Sağlamak" hedefi ile "Elektrik Dalgalanmalarını En Aza İndirmek" hedefi değerlendirmeye alınmıştır. İlk işlem olarak hedeflerin varlık katmanı riskleri ile ilişkili risk puanları hesaplanacaktır.

$$R_{PO} = \Big(\frac{\sum_{i=1}^{n}\Big(\frac{\sum_{j=1}^{m} R_{vOj} * O_{RTi}}{m}\Big)}{n} + \frac{\sum_{k=1}^{o}\Big(\frac{\sum_{l=1}^{p} R_{vOl} * O_{REk}}{p}\Big)}{o} + \frac{\sum_{t=1}^{r}\Big(\frac{\sum_{u=1}^{s} R_{vOu} * O_{RGt}}{s}\Big)}{r}\Big) N_{PS}/3$$

$$R_{PO} = \left(\left(\frac{(10{,}8 + 7{,}6 + \cdots)70 + (9{,}6 + 12{,}5 + \cdots)80 + \cdots}{mn}\right) + \left(\frac{(9{,}4 + 8{,}6 + \cdots)75 + (10{,}6 + 12{,}5 + \cdots)60 + \cdots}{po}\right) + \left(\frac{(6{,}8 + 7{,}7 + \cdots)60 + (10{,}8 + 11{,}5 + \cdots)90 + \cdots}{sr}\right)\right) 0{,}01/3 = 7{,}14(Hedef - 1)$$

$$R_{PO} = \left(\left(\frac{(11{,}6 + 8{,}4 + \cdots)80 + (8{,}6 + 9{,}8 + \cdots)90 + \cdots}{mn}\right) + \left(\frac{(8{,}4 + 11{,}6 + \cdots)85 + (11{,}6 + 8{,}3 + \cdots)70 + \cdots}{po}\right) + \left(\frac{(8{,}8 + 8{,}7 + \cdots)90 + (10{,}7 + 9{,}4 + \cdots)85 + \cdots}{sr}\right)\right) 0{,}01/3 = 8{,}88(Hedef - 2)$$

Hedeflerin risk puanlarının hesaplanmasını müteakip dolaylı etki puanlarının hesaplanması ile sistem katmanındaki hedeflerin risk hesabı yapılabilecektir. Örnek hedefler üzerinden değerlendirilecek olursa; "Elektrik Dalgalanmalarını En Aza İndirmek" hedefi "Beslenen Noktalara Kesintisiz Elektrik Sağlamak" hedefinin gerçekleşmesi açısından önemli düzeyde etkiye sahiptir. Bu değer organizasyon değerlendirmesine uygun olarak hesaplamaya dâhil edilmiştir. Benzer şekilde bütün ilişkiler irdelenmiştir.

$$D_{sO} = (\sum_{i=1}^{n} C_{Hi} \sum_{j=1}^{m} H_{öj} O_{Hj}) * N_{PS}^2/nm$$

$$D_{sO} = \Big((40 + 50 + \cdots .)\big((70 * 80) + (85 * 90) + ..\big)\Big) * \frac{0{,}01^2}{nm} = 35(Hedef - 1)$$

$$D_{sO} = \Big((60 + 55 + \cdots .)\big((80 * 60) + (95 * 70) + ..\big)\Big) * \frac{0{,}01^2}{nm} = 37(Hedef - 2)$$

$$R_{sO} = R_{PO} * D_{sO} * N_{PS}$$

$$R_{sO} = 7{,}14 * 35 * 0{,}01 = 2{,}499(Hedef - 1)$$

$$R_{sO} = 8{,}88 * 37 * 0{,}01 = 3{,}2856(Hedef - 2)$$

3) **Toplum Katmanı**: Sistem katmanında hesaplanan hedef değerleri ile kritik altyapının genel risk puanı hesabı yapılacaktır. Burada ilk olarak yine hedeflerin dolaylı etki puanı hesaplanarak genel risk puanı hesaplama aşamasına aktarılacaktır. Ülkemizde 2015 yılında gerçekleşen geniş kapsamlı ve uzun süreli elektrik kesintisinin sadece sanayiye maliyetinin milyonlarca dolar seviyesinde olduğu değerlendirilmiştir. Bu da örneğimiz üzerinden gidecek olursak "Beslenen Noktalara Kesintisiz Elektrik Sağlamak" hedefinin organizasyon dışı etkilerinin seviyesinin büyüklüğünü ve risk değeri içerisine alınma zorunluluğunu ortaya koymaktadır.

$$D_{tO} = \frac{\sum_{i=1}^{n} K_{öi} O_{Ki}}{n} * BGYS * N_{PS}^2$$

$$D_{tO} = \frac{(70 * 80) + (90 * 90) + \cdots \ldots}{n} * 80 * 0{,}01^2 = 60$$

$$R_{tO} = \frac{\sum_{i=1}^{n} H_{si} H_{öi}}{n} * D_{tO} * N_{PS}^2$$

$$R_{tO} = \frac{(2{,}4 * 80) + (3{,}2 * 90) + \cdots \ldots .}{n} * 60 * 0{,}01^2 = \mathbf{1{,}53}$$

c. Risk Yönlendirme

Elde edilen veriler, belirlenen kriterler ışığında değerlendirmeye tabi tutulduğunda genel risk puanında ve varlık risk puanlarında istenilenin üzerinde rakamlar görülmesi nedeniyle kritik altyapı üzerinde risk puanını düşürecek risk yönlendirme işlemlerinin uygulanması kaçınılmaz olarak görülür. Burada genel risk puanının %1,5 ve altı olması istenirken %1,53 olduğu, varlıklar özelinde ağ altyapısı risk puanının %10 ve altı olması istenirken %12,64 olduğu görülmektedir. Bu kapsamda yapılacak işlemler değerlendirilecek olursa;

1. Riskin tolere edilmesi varlık bazlı olarak kabul görse bile genel ve ağ altyapısı bazında tolere edilmeyeceği belirlenmiştir. Bu nedenle genel riski azaltmak adına varlık bazlı ağ altyapısı haricinde de işlemler gerekebilecektir.
2. Riske müdahale aşamasında yapılacak ilk işlem varlık katmanında zafiyet yaratan durumların önüne geçecek karşı önlem mekanizmalarının devreye alınmasıdır. Bununla birlikte personel yetkinlik seviyesinin artırılması ve BGYS organizasyonunun geliştirilmesi de önemler arasında görülmekle birlikte şu an ki hesaplamalarımızda değerlendirilmeyecektir. Varlık katmanında ağ altyapısı risk puanının düşürülmesi belirlenen kriterlere göre yapılması gereken işlemlerin ilk sırasında yer almaktadır. Bahse konu değerlerde yapılacak işlemler genel risk puanında da istenilen değere bir öteleme sağlarsa ikinci bir müdahaleye gerek kalmayacaktır. Ağ altyapısında görünen "Single Point of Failure" zafiyetine karşı alınacak bir müdahalenin eşik puanı hesabı aşağıda yer almaktadır.

$$E = (V_{DM} - (F_{KÖ} + IA)) * O_R$$
$$E = \big(35 - (10 + 6)\big) * 75 = 1425$$

Burada gerçekleştirilen müdahalede hesaplamadan görüleceği üzere risk üzerinde %75'lik bir iyileştirme söz konusu olup bu değer ağ altyapısının istenilen aralığa gelmesini sağlayacaktır. Bununla birlikte PUKÖ çevrimi kapsamında altyapı yeniden değerlendirmeye tabi tutulduğunda genel risk puanının da istenilen değere geldiği görülecektir. Bu kapsamda gerçekleştirilen müdahale risk organizasyonu tarafından değerlendirilecek yöntemler arasında yer alacaktır.

3. Riskin transfer edilmesi bir diğer azaltma yöntemleri arasında yer almakta olup burada da ilk olarak müdahale edilmesi belirlenen kriterler gereğince zorunlu olan ağ altyapısının risk transfer işlemi irdelenecektir. Risk organizasyonu tarafından veri tabanları üzerinde risk transfer işlemi uygulanmayacağının belirlenmesi nedeniyle bahse konu varlık için bu aşamada herhangi bir işlem yapılamayacaktır. Ağ altyapısının aynı zafiyeti için transfer maliyeti hesaplanırsa;

$$E = (V_{DM} - (F_{KÖ} + IA)) * O_R$$
$$E = \big(35 - (9 + 4)\big) * 60 = 1320$$

Ağ altyapısına uygulanan risk transfer yöntemi daha az maliyetli olmakla birlikte daha az etkin olduğu görülmektedir. Ancak hem varlık hem de toplum katmanındaki riskleri istenilen değerlere getirdiği görülecektir. Bu kapsamda risk organizasyonunun değerlendirmeye alabileceği yöntemlerden birisi olarak görülmektedir.

4. Risk sonlandırma işlemi genelde yüksek riskli varlıklar için uygulanmakla birlikte sistemde hesaplanan değerlere göre en riskli varlıklardan disk üniteleri üzerinde sonlandırma işlemi uygulanamayacağı kriter olarak ortaya konmuştur. Diğer varlıklar için uygulanacak sonlandırma işlemi riske müdahale kadar etkin olmayacağı için burada en uygun yöntem olarak ağ altyapısı üzerinde risk müdahalesi gözükmektedir.

ç. İzleme ve Gözden Geçirme

Bu aşamada uygulanacak iki önemli işlem mevcuttur. Bunlardan ilki uygulanan protokollerde değişme olması durumunda PUKÖ çevriminin yeniden işleterek süreci tekrardan analiz etmektir. Çünkü sistemin belirlenen risk kriterleri çerçevesinde stabil çalıştığı öngörülse de hesaplama yöntemlerindeki farklılık istenmeyen sonuçlar üretilmesine, daha net bir ifadeyle risk olmadığı değerlendirilen katmanda risk olabileceği anlamına gelmektedir. PUKÖ çevriminin yeniden işletilmesini gerektirecek diğer husus sistemin girdileridir. Mevcut durumda sistemde risk olmadığı öngörülerek çalıştığı değerlendirilse bile sistemde meydana gelecek değişimler risk puanı hesabında girdi olarak kullanılan değerlerin değişmesine ve bahse konu değişimin risk olmayan katmanda risk doğurmasına neden olabilecektir. Hâlihazırda örnek sistemimiz risk altında olduğu değerlendirilerek müdahale edilecektir. Ancak bu müdahaleyi müteakip önümüzdeki dönemlerde yukarıda belirtilen durumlar çerçevesinde risk yönlendirme işlemleri gerekebilecektir.

d. İletişim ve Danışmanlık

Kurulan risk organizasyonunun teşkilat yapısı, standarda uygunluğu ilk aşamada risk değerlendirmesine etki etmektedir. Müteakiben iş birimleri personeli yetkinlik seviyesi olarak içerik oluşturma bölümünün sistem katmanına girdi olarak eklenmiştir. Risk organizasyonunun temel birimi olan risk yönetim birimi hem organizasyon tarafından belirlenmesi gereken değerler için risk protokollerini belirlemiş hem de belirlenen protokollere uygun olarak verilerin üretilerek sisteme bağlanmasını sağlamıştır. Bununla birlikte önümüzdeki dönem içerisinde çağın gerekleri doğrultusunda risk protokollerinin değişmesi durumunu belirleyerek izleme ve gözden geçirme aşamasına gerekli girdileri yapacaktır.

Ayrıca verilen örnek üzerinde değerlendirme yapılacak olursa; risk yönetim birimi için Elektrik İletim Şirketi seviyesinde yapılacak kriter belirleme sürecine ilave üst organizasyon olan Enerji ve Tabii Kaynaklar Bakanlığı seviyesinde tüm elektrik üretim, dağıtım ve iletim sistemleri için belirlenecek kriterlerde değerlendirmeye tabi olacaktır.

4.2 Değerlendirme

Tasarlanan yapının güçlülüğü diğer çalışmalar ile olan kıyaslaması ve tasarımın doğru/etkin sonuçlar ürettiğinin doğrulaması şeklinde değerlendirmeye tabi tutulacaktır.

a. Kıyaslama

Ortaya konan çerçeve literatürdeki en önemli eksiklik olan varlık özelinde yapılan risk değerlendirmesinin kritik altyapı geneline taşınmasını sağlamıştır. Bu kapsamda kullanılan yöntemlerden katmanlı mimari sayesinde her bir katmanda ayrı risk değerlendirmesi

yapılarak ortaya çıkan riskler en alt seviyede çözümler üretilebilmektedir. Katmanlı mimari sayesinde diğer çalışmalar da yerel çözümler üretilerek sistemin bütününün görülememesi eksikliği önüne geçilmiş ve risk organizasyonu ile en temel seviyedeki iş birimleri de dâhil risk analiz ve değerlendirmesi içerisine katılmıştır. Örnek üzerinden değerlendirme yapacak olursak; önerilen yöntemle birlikte elektrik iletim yönetim sisteminin ağ altyapısında meydana gelecek bir sorunun ülkemizdeki sanayi bölgelerine vereceği zararlarında beraber değerlendirildiği bir risk analiz ve yönetim süreci yürütülmüş olacaktır.

Literatürdeki çalışmalar standartların güçlülüğünden faydalanarak değerlendirme yoluna gitmiş ancak sadece belirli standartlara uyumluluğa bakarak bahse konu standart özelinde değerlendirmeyi daraltmıştır. Çalışmamızda ihtiyaç olan bölümlerin karşılığında literatürde bir standart mevcut ise kullanılarak standartların güçlülüğün en verimli şekilde faydalanılmıştır. Bununla birlikte standart karşılığı olmayan bölümler de sistemi en iyi bilecek organizasyon tarafından perspektif şekilde tamamlanarak en etkin şekilde değerlendirmeye tabi tutulmuştur. Ayrıca çalışmanın modüler yapısı sayesinde perspektif değerlendirmeye tabi tutulan ilgili bölümler için seçilecek herhangi bir standart/çözüm/tebliğ vb. sisteme uygulanabilmektedir.

Çalışmalarda genel olarak teorik şekilde değinilen dolaylı etkiler kritik altyapıların toplum seviyesinde etkiler yaratması ve hassas bir değerlendirmeye ihtiyaç duyması nedeniyle çalışmamızda analiz içerisinde dâhil edilmiştir. Örneğimizde belirtilen "Elektrik Dalgalanmalarını En Aza İndirmek" hedefinin "Beslenen Noktalara Kesintisiz Elektrik Sağlamak" hedefine olan etki değerlendirmesi bu ihtiyacı açık bir şekilde ortaya koymaktadır.

Burada ortaya konan çalışmanın literatürdeki diğer çalışmalar karşısındaki güçlü yönlerini görmek adına Çizelge–3 üzerinde değerlendirme yapılabilecektir.

Çizelge– 3: Kıyaslama Çizelgesi

Yöntem / Özellik	Tasarlanan Çalışma	Bagheri ve Ghorbani'nin Yöntemi [25]	Romanowski ve Schneider'in Yöntemi [26]	Chen'in Yöntemi [27]	Avrupa Komisyonu Çalışması [28]	Kumaş ve Birgören'in Yöntemi [29]	Feglar ve Levy'nin Yöntemi [30]	Heo'nin Yöntemi [31]
Varlık özelinde oluşan riskin kritik altyapı geneline aktarımı veya etkilerinin görülmesi	√	x	x	x	x	x	x	x
Dolaylı etkilerin çalışmaya dâhil edilmesi	√	x	Teorik	Teorik	x	x	x	x
Bölgesel risk analizi ve yönetimi gerçekleştirme	√	Yapılabilir	x	x	Yapılabilir	x	x	x
Modüler yaklaşım(değerlemee amacıyla kullanılan yöntemlerin risk organizasyonu kararına göre değiştirilebilmesi)	√	x	x	x	x	x	x	x
Perspektif değerlendirme (Organizasyon personelinin risk değerlendirmesinde etkin rol alması)	√	√	Sınırlı	x	x	x	x	x
Risk yönetim standartlarına uyumluluk	√	x	x	x	x	Sınır	Sınır	Sınır

b. Doğrulama

Yapılan çalışmanın doğruluğu/ güçlülüğünü belirleyebilmek için analizde kullanılan verilerin belirlenme ve analiz sonuçlarının hesaplanma aşamalarını yani risk değerleme ve değerlendirme aşamalarını irdelemek gerekmektedir.

Risk değerleme aşamasında iki farklı yöntem kullanılmaktadır; standartlara uyumluluk ve

perspektif değerlendirme. Standartlar literatürde en kabul görmüş yapıyı sunması, standart ile ifade edilemeyen bölümlerin sistemi en iyi değerlendirebilecek organizasyonun perspektif değerlendirmesiyle belirlenmesi nedeniyle risk değerleme aşamasında en iyi verilerin belirlendiği aşikâr olarak görülmektedir.

Risk değerlendirme aşamasının her bir katmanında kullanılan fonksiyonlar bahse konu katmanlar için genel kabul görmüş ifadeleri ortaya koymaktadır. Ayrıca fonksiyonları oluşturan parametreler için her biri ayrı değerlendirmeye tabi tutularak literatürdeki baskın karşılıkları üretilmiştir. Nihayetinde üretilecek değer en kabul görmüş değerlendirmelere tabi olduğu için en doğru değeri vereceği kıymetlendirilmektedir.

5. Sonuç ve Öneriler

Kritik altyapıların gün geçtikçe bilgi sistemleri ile iç içe girmesi yapıyı farklı bir boyuta kaydırmaktadır. Bu durumda kritik altyapıların korunması kavramı, kritik altyapıların bilgi sistemlerinin korunması anlamına gelmektedir. Bu kapsamda, gelecek çalışmalarda kritik altyapıların siber tehditlere karşı korunması ve bu anlamda risk analizinin yapılması kritik altyapılarda risk analizi yapılması anlamı taşıyacağı değerlendirilmektedir. Bu çalışmada da bilişim altyapısında meydana gelen risklerin kritik altyapı ve diğer kritik altyapılara ne denli zararlar verebileceği gözler önüne serilmiştir.

Kritik altyapılar gün geçtikçe daha da karmaşıklaşan bir yapıya kavuşmaktadır. Bu nedenle yapılacak risk analizinin açık bir şekilde tanımlanması benzer sistemlere uygulanmasını daha da kolaylaştıracaktır. Yine bu karmaşık altyapı göz önüne alındığında varlıkların sınıflandırılması ve ilişkilerinin iyi belirlenmesi büyük önem arz etmektedir. Çünkü bir varlığa yönelen tehdit o varlığın devre dışı kalmasına veya zarar görmesine neden olmakla birlikte diğer varlıkları da önemli ölçüde etkileyebilmektedir. Ortaya konacak yaklaşımın açık ve bağlılıkları iyi göstermesi amacıyla yapılacak işlemlerin onu sistem üzerinde uygulanmasında olumsuz etkiler yaratmaması gereklidir. Çünkü açıklık ve bağlılıkların gösterimi yanı sıra yaklaşımın sistem üzerine kolay uygulanabilir olması da önemli bir kriterdir. Ayrıca önerilen yaklaşım tüm senaryoyu açık bir şekilde göz önüne sermeli ve tüm etkiler önceden rahatlıkla kestirilebilmelidir. Bu karmaşık yapı göz önünde bulundurularak hem katmanlı bir mimari tasarımı hem de senaryo tabanlı yaklaşım modelini içerecek şekilde önerilen yöntem ortaya çıkacak karmaşa kaynaklı soru işaretlerini ortadan kaldıracağı gibi istenilen tüm kritik altyapılara da kolay bir şekilde uygulanabileceği değerlendirilmektedir.

Bu kapsamda yukarıda belirttiğimiz katmanlı mimari ve senaryo tabanlı yaklaşıma ilave varlık tabanlı kabul görmüş risk analiz ve yönetim yöntemleri ile konuya ilişkin uluslararası standart/prosedür/çerçeveler harmanlanarak bahse konu yöntem ortaya konmuştur. Bu yöntemle genel olarak yeni bir risk analiz ve yönetim yaklaşımı yerine mevcut kabul görmüş literatürü kritik altyapılar üzerine kolay ve etkin bir şekilde uygulama amaçlanmıştır.

Gerçekleştirilen analiz sonucunda; risk analiz ve yönetiminde ihtiyaç duyulan gereklilikler ile konu üzerine yapılan çalışmaların ihtiyaca uygun ve güçlü olduğu değerlendirilen yönleri ile karşılanabilecek düzeyde bir tasarım ortaya konduğu görülmüştür. Tasarımda perspektif yaklaşım ile standartlara uyumluluk arasında bir denge gözetilmekle birlikte kritik altyapıya özgü değişkenlerin perspektif yaklaşımla, genel değişkenlerin standartlar üzerinden belirlenmesi usulü baz alınmıştır. Ancak bazı değerler genel değişken olarak değerlendirilmekle birlikte tam ve etkin bir standart tarafından belirleme usulü ortaya konamadığı için perspektif yaklaşımla değerlendirilmek zorunda kalınmıştır. Önümüzdeki çalışmalarda tasarım geliştirilmesinde en önemli ilerleme noktasının tüm genel değişkenlerin belli standartlar üzerinden sağlanması olduğu kıymetlendirilmektedir.

Kaynakça

[1] Gandhi R., Sharma A., Mahoney W., Sousan W., Zhu Q, Laplante P., Dimensions of Cyber-Attacks, IEEE Technology and Society Magazine, vol.30, issue.1, pp.28-38, Spring 2011.

[2] CEC, 2004, Critical Infrastructure Protection in the Fight Against Terrorism, Commission of the European Communities.

[3] BTK, 2011, Kritik Altyapıların Korunması Belgesi, Bilgi Teknolojileri ve İletişim Kurumu.

[4] UDHB, 2015, 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi, Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

[5] AFAD, 2014, 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi, Afet ve Acil Durum Yönetimi Başkanlığı.

[6] Beggs P., Securing the Nation's Critical Cyber Infrastructure, US Department of Homeland Security, February 2010.

[7] Jung-Ho E., Nam-Uk K., Sung-Hwan K., Tai-Myoung C., Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare, International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 2012.

[8] OECD, 2008, Working Party on Information Security and Privacy, Recommendations of the Council on the Protection of Critical Information Infrastructures, Organisation for Economic Co-operation and Development.

[9] TSE, 2002, Bilgi Teknoloji-Bilgi Güvenliği Yönetimi İçin Uygulama Prensipleri, TS ISO/IEC 17799, Türk Standartları Enstitüsü.

[10] ISO, 2005, 27001 Information Security Management System, International Organization for Standardization.

[11] ISO, 2009, 31010 Risk Assessment Techniques, International Organization for Standardization.

[12] ANSI, 2011, Z690.3 Risk Assessment Techniques, American National Standards Institute.

[13] Security Service on behalf of the UK Government, CRAMM Management Guide, first published April 1996.

[14] C&A System Security Limited. COBRA consultant products for Windows. Evaluation & User Guide, 2000.

[15] Soğukpınar İ., Karabacak B., ISRAM: information security risk analysis method, Elsevier Computer & Security, vol. 24, issue.2, pp. 147-159, March 2005.

[16] Christopher Alberts, Audree Dorofee, CarolWoody_Carnegie Mellon University, Introduction to the OCTAVE Approach, is sponsored by the Department of Defense, August 2003.

[17] [Kailey MP, Jarratt P. RAMEX: a prototype expert system for computer security risk analysis and management. Computers& Security, 14(5):449-63, 1995.

[18] Bilbao A. TUAR. A model of risk analysis in the security field, CH3119-5/92.IEEE, 1992.

[19] Paulina J., Marek P., "Designing a Security Policy According to BS 7799 Using the OCTAVE Methodology", Second International Conference on Availability, Reliability and Security (ARES'07), 2007.

[20] Yong Q, Long X. Qianmu L., Information security risk assessment method based on CORAS frame, International Conference on Computer Science and Software Engineering, 12-14 December 2008.

[21] Sarkheyli A., Ithnin N.B., Improving the current risk analysis techniques by study of their process and using the human body's Immune System", 5th International Symposium on Telecommunications, 4-6 December 2010.

[22] ISO, 2009, 31000 Risk Management – Principles and Guidelines, International Organization for Standardization.

[23] ISO, 2011, 27005 Information Security Risk Management, International Organization for Standardization.

[24] NIST, 2011, 800-39 Managing Information Security Risk, National Institute of Standards and Technology.

[25] Bagheri E., Ghorbani A.A., Risk Analysis in Critical Infrastructure Systems based on the Astrolabe Methodology, Fifth Annual Conference on Communication Networks and Services Research, 2007.

[26] Romanowski C., Schneider J., Critical Infrastructure protection and risk analysis in the mid-size city, IEEE Conference on Technologies for Homeland Security, 13-15 November 2012.

[27] Chen K.Y., Heckel-Jones C.A.C., Maupin N.G., Rubin S.M., Bogdanor J.M., Guo Z., Haimes Y.Y., Risk Analysis of GPS-Dependent Critical Infrastructure System of Systems, Systems and Information Engineering Design Symposium, 25 April 2014.

[28] Giannopoulos G., Filippini R, Schimmer M., Theocharidou M., Risk Assessment Methodologies for Critical Infrastructure Protection, European Commission Joint Research Centre Institute for Protection and Security of the Citizen, Part – I EUR 25286 EN – 2012, Part – II EUR 27332 EN – 2015.

[29] Kumaş E., Birgören B., E-Devlet Kapısı Projesi Bilgi Güvenliği ve Risk Yönetimi: Türkiye Uygulaması, Bilişim Teknolojileri Dergisi, Cilt.3, Sayı.2, Sayfa.29-36, Mayıs 2010.

[30] Feglar T., Levy J.K., Protecting Cyber Critical Infrastructure (CCI): Integrating Information Security Risk Analysis and Environmental Vulnerability Analysis, IEEE International Engineering Management Conference, 18-21 October 2004.

[31] Heo J., Shin J.W., Lee W., Won Y., Risk Analysis Methodology for New Critical Information Infrastructure, Third International Conference on Systems and Networks Communications, 26-31 October 2008.

[32] Sierla S., Hurkala M., Charitoudi K., Security Risk Analysis for Smart Grid Automation, IEEE 23rd International Symposium on Industrial Electronics, 1-4 June 2014.

[33] Yasakethu S.L.P., Jiang J., Graziano A., Intelligent Risk Detection and Analysis Tools for Critical Infrastructure Protection, IEEE Eurocon, 1-4 July 2013.

[34] Guzman A., Ishida S., Choi E., Aoyama A., Artificial Intelligence Improving Safety and Risk Analysis: A Comparative Analysis for Critical Infrastructure, IEEE International Conference on Industrial Engineering and Engineering Management, 4-7 December 2016.

[35] NIST, 2014, Framework for Improving Critical Infrastructure Cyber Security, National Institute of Standards and Technology.

[36] Arno R.G., Stoyas E., Schuerger R., Risk Analysis for NEC Article 708 Critical Operations Power Systems, IEEE Industry Applications Society Annual Meeting, 4-8 October 2009.

[37] Hua J., Bapna S., The Economic Impact of Cyber Terrorism, Elsevier The Journal of Strategic Information Systems, vol.22, issue.2, pp.175-186, June 2013.

[38] Park W.H., Risk Analysis and Damage Assessment of Financial Institutions in Cyber Attacks between Nations, Elsevier Mathematical and Computer Modelling, vol.58, issue.11-12, pp.1845, December 2013..