T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KRİTİK ALTYAPILARDA SİBER RİSK ANALİZİ VE YÖNETİMİNE YÖNELİK ÇERÇEVE ÖNERİSİ

EMRE KIRAN
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

GEBZE
2021

T.C.
GEBZE TEKNİK ÜNİVERSİTESİ
FEN BİLİMLERİ ENSTİTÜSÜ

KRİTİK ALTYAPILARDA SİBER RİSK ANALİZİ VE YÖNETİMİNE YÖNELİK ÇERÇEVE ÖNERİSİ

EMRE KIRAN
YÜKSEK LİSANS TEZİ
BİLGİSAYAR MÜHENDİSLİĞİ ANABİLİM DALI

DANIŞMANI
PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE
2021

T.R.

GEBZE TECHNICAL UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES

FRAMEWORK PROPOSAL FOR CYBER RİSK ANALYSIS AND MANAGEMENT IN CRITICAL INFRASTRUCTURE

EMRE KIRAN

A THESIS SUBMITTED FOR THE DEGREE OF MASTER OF SCIENCE

DEPARTMENT OF COMPUTER ENGINEERING

THESIS SUPERVISOR

PROF. DR. İBRAHİM SOĞUKPINAR

GEBZE

2021

GEBZE TEKNİK ÜNİVERSİTESİ	YÜKSEK LİSANS JÜRİ ONAY FORMU

GTÜ Fen Bilimleri Enstitüsü Yönetim Kurulu'nun 01/07/2021 tarih ve 2021/30 sayılı kararıyla oluşturulan jüri tarafından 28/07/2021 tarihinde tez savunma sınavı yapılan Emre KIRAN'ın tez çalışması Bilgisayar Mühendisliği Anabilim Dalında YÜKSEK LİSANS tezi olarak kabul edilmiştir.

JÜRİ

ÜYE
(TEZ DANIŞMANI) : PROF.DR.İBRAHİM SOĞUKPINAR

ÜYE : PROF.DR.ALİ GÖKHAN YAVUZ

ÜYE : DOÇ.DR.MEHMET GÖKTÜRK

ONAY

Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Yönetim Kurulu'nun
…..…/…..…/..…… tarih ve ……/……... sayılı kararı.

İMZA/MÜHÜR

ÖZET

Toplum sağlığı ve ekonomisi ile kamu güvenliği üzerinde ciddi etkileri olan varlık ve sistemlerden oluşan yapılar bütünü, fonksiyonlarını kısmi veya tamamıyla yitirmesi durumunda kamu hizmetlerinin yürütülmesi ile toplumsal düzeni olumsuz etkilemesi nedeniyle kritik altyapı olarak değerlendirilmektedir. Bahse konu yapıların hayati önemi nedeniyle korunması ve bunu sağlayabilmek için varlık değerinin ortaya konarak hangi riskleri taşıdığının tespit edilmesi gerekmektedir. Bu kapsamda yapılacak çalışmalar risk analizi olarak değerlendirilmekte olup, risk analizi kritik altyapıların kısmi veya tamamıyla devre dışı kalmasının olası etkileri ve zayıf noktalarını değerlendirebilmek için olumsuz durum senaryolarının ortaya konmasıdır. Konunun öneminin gün geçtikçe artması nedeniyle hem ülkeler hem de uluslar arası kuruluşlar tarafından standartların belirlenmesi, koruma çerçeveleri oluşturulması çalışmaları hız kazanmıştır. Söz konusu standart ve koruma çerçevelerinin, risk analizi ve yönetimine yönelik oluşturulacak veri setlerinde önemli bir referans olacağı görülmüş ve bunlardan faydalanarak kritik altyapıların korunması, risk analizi ve yönetiminin yapılmasına yönelik bir çatı önerilmiştir. Ayrıca ortaya konan çatının, kritik altyapılara yönelik özelleşmesi için literatürde kabul görmüş çalışmaların güçlü yönlerinden faydalanılmıştır. Risk analizi ve yönetimi çalışmalarına yönelik kurulan çatı modellerinin, en kabul görmüş değerlendirme yöntemi olan jenerik bir senaryo üzerinden vaka çalışması yapılarak sonuçlar ortaya konmuştur. Sonuçlar, dolaylı etkileri ile birlikte tüm aşamaları içerisine alarak değerlendirme yapmayı sağlayacak bir çatı oluşturulduğunu ve çatının her katman için ayrı değerlendirme imkânı sunduğunu göstermiştir. Bununla birlikte çatının modüler yapısı sayesinde değişen standart ve çerçevelerin hızlı bir şekilde yapıya dâhil edilebileceği de görülmüştür.

Anahtar Kelimeler: Risk Analizi, Kritik Altyapılar, Katmanlı Mimari, Senaryo Tabanlı Yaklaşım, Risk Yönetim Standartları, Perspektif Risk Yaklaşımı.

SUMMARY

Structures consisting of assets and systems that have serious effects on public health, economy, and public safety are considered as critical infrastructure, as they adversely affect the execution of public services and social order in case of partial or complete loss of their functions. Due to the vital importance of the mentioned structures, it is necessary to protect them and in order to achieve this, it is necessary to determine the risks they carry by revealing the asset value. The studies to be carried out in this context are evaluated as risk analysis, and risk analysis is the revealing of adverse situation scenarios in order to evaluate the possible effects and weak points of partial or complete failure of critical infrastructures. 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. It has been seen that the said standards and protection frameworks will be an important reference in the data sets to be created for risk analysis and management, and a framework has been proposed for the protection of critical infrastructures, risk analysis and management by taking advantage of them. In addition, the strengths of the studies accepted in the literature were used to privatize the revealed framework for critical infrastructures. A case study was conducted over a generic scenario, which is the most accepted evaluation method for the framework models established for risk analysis and management studies, and the results were presented. The results show that a framework has been created that will allow evaluation by taking into account all the stages together with its indirect effects, and that the framework offers an opportunity to evaluate separately for each layer. However, thanks to the modular structure of the framework, it has been observed that changing standards and frames can be quickly incorporated into the structure.

Key Words: Risk Analysis, Critical Infrastructures, Layered Architecture, Scenario-Based Approach, Risk Management Standards, Perspective Risk Approach.

TEŞEKKÜR

Lisansüstü eğitimimin başlangıcından itibaren hem ders aşamasında hem de tez konusunun belirlenip nihai olarak bu çalışmanın ortaya konmasına kadar geçen süreçte yardım ve desteklerini hiçbir zaman esirgemeyip, bilgisi, tecrübesi ve yol göstericiliği ile yanımda olan değerli tez danışmanım sayın Prof. Dr. İbrahim SOĞUKPINAR başta olmak üzere böyle bir çalışma gerçekleştirebilecek eğitim seviyesine ulaşmamda katkısı olan ilkokul birinci sınıftan itibaren üzerimde emeği geçen tüm hocalarıma,

Bütün çalışmam boyunca, lisansüstü eğitimimin başarıyla tamamlanabilmesi amacıyla destekleri ile birlikte bilgi ve tecrübelerini benimle paylaşan saygıdeğer birim amirlerime,

ve çalışmamın başarı ile ortaya konmasındaki en büyük manevi desteği sağlayan başta sevgili eşim Demet KIRAN olmak üzere tüm aileme en içten teşekkürlerimi sunarım.

İÇİNDEKİLER

	Sayfa
ÖZET	v
SUMMARY	vi
TEŞEKKÜR	vii
İÇİNDEKİLER	viii
SİMGELER ve KISALTMALAR DİZİNİ	x
ŞEKİLLER DİZİNİ	xi
TABLOLAR DİZİNİ	xii
1. GİRİŞ	1
1.1. Tezin Amacı, Katkısı ve İçeriği	2
2. KRİTİK ALTYAPILARIN KORUNMASI	4
2.1. Kritik Altyapılar	4
2.1.1. Kritik Altyapılara Küresel Bakış Açısı	5
2.1.2. Kritik Altyapılar ve Bilgi Teknolojileri	8
2.2. Siber Güvenlik	8
2.2.1. Kritik Altyapılarda Siber Güvenliği İyileştirme Çerçevesi	9
2.2.2. ENISA Ulusal Siber Güvenlik Stratejileri Raporu	10
2.2.3. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı	10
2.3. Risk Analizi ve Yönetimi	11
2.3.1. ISO 31000 Risk Yönetimi	13
2.3.2. ISO 31010 Risk Değerlendirme Teknikleri	14
2.3.3. ISO 27005 Bilgi Güvenliği Risk Yönetimi	14
2.3.4. NIST 800 – 39 Bilgi Güvenliği Riskini Yönetme	15
2.4. Konu Üzerine Yapılan Çalışmalar	15
3. KRİTİK ALTYAPILARDA SİBER RİSK ANALİZİ VE YÖNETİMİNE YÖNELİK ÇERÇEVE ÖNERİSİ	19
3.1. Önerilen Çerçeve Tasarımı	20
3.1.1. İçerik Oluşturma	21
3.1.2. Risk Değerlendirmesi	32
3.1.3. Risk Yönlendirme	33

3.1.4. İzleme ve Gözden Geçirme 34
3.1.5. İletişim ve Danışmanlık 35
4. VAKA ÇALIŞMASI VE DEĞERLENDİRME 36
4.1. Vaka Çalışması 36
4.1.1. İçerik Oluşturma 36
4.1.2. Risk Değerlendirmesi 38
4.1.3. Risk Yönlendirme 42
4.1.4. İzleme ve Gözden Geçirme 44
4.1.5. İletişim ve Danışmanlık 45
4.2. Değerlendirme 45
4.2.1. Kıyaslama 45
4.2.2. Doğrulama 47
5. SONUÇLAR, ÖNERİLER VE GELECEK ÇALIŞMASI 49

KAYNAKLAR 51
ÖZGEÇMİŞ 55
EKLER 56

SİMGELER ve KISALTMALAR DİZİNİ

Simgeler ve Kısaltmalar		**Açıklamalar**
AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
AFAD	:	Afet ve Acil Durum Yönetimi Başkanlığı
ANSI	:	American National Standards Institute
BM	:	Birleşmiş Milletler
COBRA	:	CO-Benefits Risk Assessment
CRAMM	:	CCTA Risk Analysis and Management Method
ENISA	:	The European Union Agency for Cybersecurity
GPS	:	Global Positioning System
IEC	:	The International Electrotechnical Commission
ISO	:	International Organization for Standardization
ISRAM	:	Information Security Risk Analysis Method
ITU	:	The International Telecommunication Union
ITU-T	:	The ITU Telecommunication Standardization Sector
NATO	:	North Atlantic Treaty Organization
NIST	:	National Institute of Standards and Technology
OCTAVE	:	The Operationally Critical Threat, Asset, and Vulnerability EvaluationSM
PUKÖ	:	Planla, Uygula, Kontrol Et, Önlem Al
RAMEX	:	Risk Analysis and Management Expert System
SCADA	:	Supervisory Control and Data Acquisition
TUAR	:	Unified Theory of Risk Analysis

ŞEKİLLER DİZİNİ

Şekil No:		Sayfa
2.1:	ABD Kritik Altyapıları.	5
2.2:	Türkiye Kritik Altyapıları.	7
2.3:	Risk Yönetimi.	12
3.1:	Kritik Altyapılarda Siber Risk Analizi ve Yönetimi Çerçevesi Modeli.	20
3.2:	Kritik Altyapılarda Siber Risk Analizi ve Yönetimi Çerçevesi Model Adımları.	21
3.3:	Sistem Gereklilikleri Şablonu.	22
3.4:	Senaryo Tabanlı Yaklaşım Modeli.	23
3.5:	Belirlenecek Değerler ve Risk Değerlendirme Teknikleri.	30
4.1:	Risk Protokolleri.	37

TABLOLAR DİZİNİ

Tablo No:		**Sayfa**
3.1:	Semboller Tablosu – 1.	24
3.2:	Bilgi Güvenliği Değerlendirme Matrisi.	24
3.3:	Semboller Tablosu – 2.	25
3.4:	Semboller Tablosu – 3.	26
3.5:	Semboller Tablosu – 4.	27
3.6:	Semboller Tablosu – 5.	28
3.7:	Semboller Tablosu – 6.	29
3.8:	Semboller Tablosu – 7.	30
3.9:	Belirlenecek Değerler.	31
3.10:	Semboller Tablosu – 8.	33
4.1:	Kıyaslama Tablosu.	46

1. GİRİŞ

Günümüzde internetin kelime karşılığı olarak kullanılan siber uzay terimi, bilgisayarlar ve onu kullanan insanların birbirleri arasında kurduğu iletişimdeki sanal gerçeklik olarak ifade edilebilmektedir. İlk defa Kanadalı ünlü bilim kurgu yazarı William Gibson tarafından Neuromancer adlı romanda siber uzay kavramı kullanılmıştır. Genellikle sanal kavramı ile karıştırılan siber kavramı ilk olarak Louis Couffignal tarafından 1958 yılında kullanılmıştır. Her iki kavram internet için geçerli olan önermelerdir. İletişim bakımından siber, sunduğu ortam bakımından sanal olan internet gün geçtikçe üstel olarak büyüyen bir mecra haline gelmiştir. Günümüzde aktif internet kullanıcı sayısı 4,5 milyarı aşmıştır. Bunun anlamı dünya nüfusunun yaklaşık olarak % 60'ı çeşitli nedenlerle internet ortamına dâhil olmaktadır. Microsoft tarafından yapılan küresel siber risk algısı araştırmasında [1] kurum ve kuruluşların önümüzdeki dönemde % 90 oranında Bulut Bilişim, % 74 oranında Nesnelerin İnterneti teknolojilerine yönelmeyi düşündüğü göz önüne alındığında internet ortamının daha da büyüyeceği açık bir şekilde görülmektedir. Bilişim teknolojilerinin sağlamış olduğu imkânlardan faydalanmak isteyen kurum ve kuruluşlar tüm altyapılarına hızlı bir şekilde söz konusu teknolojileri uyarlayıp yaygınlaştırılmalarını sağlamaktadır.

Büyük bir mecra halini alan internet ortamı beraberinde büyük güvenlik risklerini de getirmektedir. Kaspersky tarafından yayınlanan güvenlik bülteninde [2] sadece son bir yıl içerisinde bir milyar civarında atak tespit edildiği raporlanmıştır. Symantec tarafından yayınlanan güvenlik tehditleri raporunda [3] ise internet adreslerinin yaklaşık % 10'unun zararlı olduğu, son bir yılda web ataklarının % 56 oranında, bunun içerisinde tedarik zinciri ataklarının ise % 78 oranında arttığı vurgulanmıştır. Ayrıca günlük web sitesi kırma sayısının 190.000 civarına ulaşması [4], Kaspersky tarafından yapılan bir güvenlik araştırmasında da [5] insanların internet ortamını özellikle Facebook, Twitter, Instagram, e-mail vb. üzerinden haberleşme, bankacılık ve ödeme işlemleri ile çevrimiçi alışveriş amacıyla kullandığını göstermesi de bu raporu destekler niteliktedir. Diğer tarafından Microsoft tarafından yapılan araştırma da [1] şirketlerin % 59 ile ekonomik belirsizliğin önünde kendileri için en önemli tehdit olarak % 79 ile siber tehditleri gördüğünü, bununda internet ortamındaki güvenlik riskleri konusunda önemli bir farkındalık oluştuğunu göstermiştir.

1.1. Tezin Amacı, Katkısı ve İçeriği

Son yıllarda gerçekleşen siber saldırıların özellikle kritik altyapılara yöneldiği, bunun en önemli nedeni olarak siber silahların geleneksel silahlara nazaran daha düşük maliyetli olması ve daha büyük zararlar vermesi olduğu görülmektedir. Ayrıca siber saldırıların kaynaklarının tespitinin de çok zor olması önemli bir tercih sebebi olmaktadır.

Kamu hizmetlerinin devamlılığı ve toplum düzeninin sağlanması, kritik altyapıların tanımına bakıldığında da esas alındığı açık olarak görülmektedir. Bu noktadan hareketle, kritik altyapılar daha geniş çerçevede; "Fonksiyonlarını kısmi veya tamamıyla yitirmesi durumunda kamu hizmetlerinin yürütülmesi ile toplumsal düzeni olumsuz etkilemesi nedeniyle, toplum sağlığı ve ekonomisi ile kamu güvenliği üzerinde ciddi etkileri olan varlık ve sistemlerden oluşan yapılar bütünü" şeklinde tanımlanabileceği değerlendirilmektedir. 1990'ların başından bu yana, kritik altyapı bileşenlerinde kullanılan tescilli, fiziksel bağlantılı otomasyon sistemlerinin yerini modern SCADA sistemleri almıştır [6]. Kapsamlı ve bütünleşik bir SCADA sistemi sayesinde bir tesise ait tüm sistemlerin izleme, kontrol, veri toplama, veri kaydı ve saklanması başta olmak üzere ana ve yardımcı işletmelerdeki çevre kontrol birimlerinin otomatik kontrol ve gözlemlenmesi sağlanabilmektedir. Her geçen gün bilgi ve iletişim teknolojisinin sağladığı faydalar daha fazla oranda kritik altyapı sistemleriyle bütünleşmektedir. Bu gelişmeler kritik altyapılardaki fiziksel koruma stratejisinin mantıksal koruma stratejisine evirilmesine neden olmuş ve kritik bilgi altyapısı kavramının ortaya çıkmasını sağlamıştır. Bu kapsamda gerçekleştirilen çalışma kritik altyapıların temelini teşkil eden kritik bilgi altyapılarına odaklanmıştır.

Kuruluşların işleyişlerini etkileyen risklerin belirli norm ve yöntemlere uygun şekilde tanımlanması, kıymetlendirilmesi ve gerekli kontrollerin, politika ve yordamların hayata geçirilmesi ile muhtemel kayıpların önüne geçilmesi ya da azaltılması, izlenmesi ve gözden geçirilmesi olarak ifade edilen risk analizi ve yönetimi, bilgi ve iletişim teknolojilerindeki güvenliğin ilk adımı olarak görülmektedir. Kritik altyapıların korunmasına yönelik yapılacak tüm çalışmaların temelinde de kritik bilgi altyapılarına yönelik yapılacak risk analiz ve yönetim çalışmaları olması gerektiği değerlendirilmektedir.

Risk Analiz ve Yönetiminde en kabul görmüş çalışmalar, birçok metodoloji/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 metodoloji/teknik/standart/model/çerçeve irdelenerek kritik altyapıların korunmasına yönelik en önemli adımlardan birine yönelik bir çerçeve tasarımı oluşturulmuştur.

Bu tez kapsamında, öncelikle ikinci bölümde siber güvenliğe yönelik genel bakış açısıyla birlikte oluşturulacak çatıya temel teşkil edecek dokümanlar, koruma stratejilerinin temelinde yer alan risk analizi ve yönetimine yönelik konu üzerinde yapılan çalışmalar ve çatının kurulumunda faydalı olabilecek yöntemler ele alınmıştır. Üçüncü bölümde çatı tasarımı ortaya konarak dördüncü bölümde ortaya konan çatı, bir vaka çalışması üzerinde gerçeklenmiştir. Beşinci ve son bölümde ise elde edilen sonuçlar ve sonuçlar ile ilgili öneriler ve gelecek önerileri konu başlıkları altında anlatılmıştır.

2. KRİTİK ALTYAPILARIN KORUNMASI

Ülkeler için önemi göz önüne alındığında kritik altyapıların korunması her dönem için çok önemli bir faaliyet olmuştur. Kritik altyapılara yönelik bakış açıları değerlendirilecek olursa, zaman içinde teknolojik gelişmeler ile birlikte odak noktasının fiziksel bir korumadan mantıksal bir korumaya doğru kaydığı görülecektir. Bu çerçevede koruma stratejilerinin ortaya konması, korumanın ilk adımını oluşturan risk analiz ve yönetimine yönelik önemli veri setlerinin oluşmasını sağlayacaktır. Kritik altyapıların korunması, ülke güvenliği açısından ayrı bir öneme sahip olduğu gibi kritik altyapılara yönelik risk analizi ve yönetimi çalışmalarının da genel değerlendirmelerden ayrı düşünülmesi gerektiği kıymetlendirilmektedir. Bununla birlikte genel değerlendirme ve literatür çalışmalarının kritik altyapılara yönelik yapılacak risk analiz ve yönetimi çalışmaları için temel teşkil edeceği görülmektedir.

2.1. Kritik Altyapılar

Son yıllarda kritik altyapılara yönelik gerçekleştirilen siber saldırı ve olaylar ile kritik altyapıları etkileyen doğal afetler, başta ülkeler olmak üzere birçok kurum ve kuruluşun güvenlik kavramını yeniden değerlendirmesine neden olmuştur. Gerçekleşen siber saldırıların amaçları bakımından politik, sosyo-kültürel ve ekonomik [7] 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 vatandaşların huzuru ve ülkenin güvenliği bakımından hayati öneme haiz altyapıların belirlenmesi ve koruma stratejilerinin ortaya konulması hususunda ciddi bir görüş birliği oluşmasına neden olmuştur.

Kritik altyapılar ile ilgili tanımların temel olarak, kamu hizmetlerinin devamlılığı ile toplum düzeninin sağlanması üzerine oturduğu görülmektedir. Bu noktadan hareketle, kritik altyapılara yönelik tanımlar farklılık göstermekler birlikte genel olarak; “Sahip olduğu bilişim sistemleri üzerinde işlenen bilginin/verinin temel bilgi güvenliği kriterleri açısından bozulması durumunda insan hayatına, ciddi maddi kayıplara, ulusal güvenlik risklerine veya kamu düzeninin bozulmasına neden

olabilecek altyapılar”[8] şeklinde tanımlanabileceği değerlendirilmektedir. Kritik altyapıların tanımı gibi kapsamı da ülkeden ülkeye değişmektedir.

2.1.1. Kritik Altyapılara Küresel Bakış Açısı

2004 yılında AB Komisyonu tarafından ortaya konan “702 sayılı Terörizmle Mücadele Kapsamında Kritik Altyapıların Korunması” konulu tebliğde [9] “Kritik altyapı:...insan hayatı, sosyal ilişkiler, toplum sağlığı, emniyeti ve güvenliği ile ekonomik ve toplumsal refah açısından ihtiyaç duyulan ve zarar görmesi veya ortadan kalkması durumunda söz konusu ihtiyaçların karşılanmasında ciddi zafiyetler doğuracak varlık, sistem ve bunların bağlantılı üniteleri” şeklinde tanımlanmıştır. ABD mevzuatında “kritik altyapı” tanımı; “İşleyemez duruma gelmesi veya yok edilmesi durumunda, ulusal güvenlik, ekonomi, kamu sağlığı ve emniyeti ile bunların birleşimi üzerinde ciddi etkileri olan ABD için hayati öneme sahip fiziksel veya sanal sistem/varlıklar” şeklindedir [10]. Kritik altyapıların korunmasını ulusal güvenlik kapsamında değerlendiren ABD hükümeti, “Ulusal Altyapı Koruma Planı”nda[11] kritik altyapılara yer vermiştir. Bu planda, ABD’ye ait 18 adet kritik altyapı şekil 2.1'de [11] belirtilmiştir.

	Tarım ve Gıda		Bankacılık ve Finans		Kimya
	Ticari Tesisler		İletişim		Kritik Üretim
	Barajlar		Savunma Sanayi		Acil Servisler
	Enerji		Hükümet Tesisleri		Sağlık Hizmeti ve Kamu Sağlığı
	Bilgi Teknolojisi		Ulusal Anıtlar ve Simgeler		Nükleer Reaktörler, Maddeler ve Atıklar
	Posta ve nakliye		Ulaşım Sistemleri		Su

Şekil 2.1: ABD Kritik Altyapıları.

AB'nin ABD ile kıyaslandığında kritik altyapıların korunmasına yönelik bakış açıları farklılık göstermektedir. AB konuya üye ülkelerinde yer alan vatandaşların sağlığı ve emniyeti ile toplumsal güvenlik ve ekonomik refah açısından değerlendirerek üye ülkelerin söz konusu normlara yönelik korunması açısından bakmaktadır. AB Konseyi'nin kritik altyapı olarak değerlendirdiği yapılar:

- Sağlık (Hastaneler, araştırma merkezleri vb.)
- Finans (Ekonomi kuruluşları, bankalar vb.)
- Enerji (Enerji üretim ve dağıtım tesisleri vb.)
- Ulaşım (Otoyollar, demiryolları, havaalanları vb.)
- Kimyasal, Biyolojik, Radyoaktif ve Nükleer madde endüstrisi
- Su (Şebekeler, barajlar vb.)
- Gıda (Üretim, depolama vb.)
- Bilgi ve İletişim (İnternet altyapısı, haberleşme vb.)
- Kamu düzeni ve güvenlik
- Uzay araştırmaları
- Sivil yönetim

Ülkemizdeki kritik altyapıların korunması çalışmaları incelenecek olursa, önümüzdeki yıllarda siber güvenlik çalışmalarının, gelinen durum itibariyle siber güvenlik stratejileri doğrultusunda ana temasının "kritik altyapıların korunması" olacağı değerlendirilmektedir. Bu kapsamda ülkemizde yapılan en önemli çalışmaların başında Ulusal Siber Güvenlik Stratejisi ve Eylem Planı gelmektedir. Gerek strateji belgesinin amacı ve kapsamı gerekse eylem maddeleri çok büyük oranda "kritik altyapıların korunması" temasının altını doldurmaktadır. Bununla birlikte kritik altyapıların önemini Şekil – 2.2'de [12] yer alan görselle ifade eden AFAD'ın koordinasyonunda hazırlanan 2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi'nde [12] "Son yıllarda artan terör tehdidiyle ve yaşanan büyük çaplı felaketler ülkeleri kritik altyapıların korunmasıyla ilgili politika, strateji, mevzuat, plan ve programlar yapmaya itmektedir" denilerek, alınması gereken bazı önlemler sıralanmıştır:

- Bütün bakanlıklar kritik altyapıların belirlenmesi" için 2'şer personel belirleyecek,
- Enerjiden ulaştırmaya, su yönetiminden haberleşmeye kadar sektörlerde ‘yetkili otorite’ tespit edilecek,
- Boru ve ulaştırma hatları nedeniyle uluslararası boyut da göz önüne alınarak AB'yle grup oluşturulacak,
- Koruyucu tedbirleri artırıcı yasal düzenlemeler ve yönetmelikler hazırlanacak,
- Büyük tehdit senaryoları göz önüne alınarak, her bir altyapının zayıf noktaları için risk analizi yapılacak,
- Özel işletmeler ile devlet otoritesi arasında ‘güvenlik irtibat görevlisi’ atanacaktır.

Şekil 2.2: Türkiye Kritik Altyapıları.

Bunlar haricinde de dünyada ülkeler, NATO, BM gibi önemli kuruluşlar ve hatta sivil firmalar dâhil konuya yönelik politikasını belirlememiş bir organizasyon neredeyse kalmamıştır.

2.1.2. Kritik Altyapılar ve Bilgi Teknolojileri

Bilgi ve iletişim teknolojilerinin gün geçtikçe artan kullanımı kritik altyapı kavramının daha yüksek sesle dile getirilmesini sağlamıştır. Toplumsal yaşamda birçok altyapının temeli/sürdürülmesi kritik altyapılara bağlı olduğu gibi, bilgi çağında kritik altyapıların temelinde de siber/bilişim altyapıları yer almaktadır [13][14]. Bilgi ve iletişim teknolojilerinin sağlamış olduğu imkanlar kritik altyapı yönetimini kolaylaştırmak ve geliştirmek adına her geçen gün daha fazla önem kazanmaktadır. Bu durum, kritik altyapıların daha geniş çerçevede "kritik bilgi altyapıları" olarak anılmasına neden olmaktadır. OECD, işlevlerini yitirmesi durumunda toplum sağlığı, güvenliği ve emniyeti ile ekonomik refah ve verimliliğe önemli ölçüde etki eden bilgi sistemleri ve ağlarını kritik bilgi altyapıları olarak tanımlamaktadır [15]. Bu kapsamda gerçekleştirilen çalışma kritik altyapıların temelini teşkil eden kritik bilgi altyapılarına odaklanmıştır.

2.2. Siber Güvenlik

Siber güvenlik, siber uzayda işlenen bilginin/verinin bilgi güvenliği normları açısından güvence altına alınması, altyapıları oluşturan bilgi sistemlerinin saldırılardan korunması, tespit mekanizmalarının üretilmesi, tespitlere karşı önlem mekanizmalarının devreye alınması ve geri kurtarma yordamlarının uygulanmasını içeren faaliyetler bütünüdür. Dünya üzerindeki erişim kolaylıkları nedeniyle siber tehditler herhangi bir noktadan gelebilmektedir. Bu nedenle siber güvenlik milli güvenlikten ayrı olarak düşünülemez.

Son dönemde yaşanan ülkeler arasındaki gerginlikler ve küresel salgın ortamı, teknolojik dönüşümü hızlandırmış ve buna paralel olarak toplumsal ve ekonomik yaşantının siber ortama bağımlılığını daha da artırmıştır. Gelinen durumda ülkelerin ekonomik büyümesinde siber güvenliğe yapılacak yatırımlar önemli rol oynamaya başlamıştır. Siber güvenliğin hem ulusal hem de uluslararası güvenlik kapsamı içerisinde önemli bir yer tutmasının temel nedenlerinden birisi de büyüyen siber ortamın kritik altyapıları da içerisine alması olmuştur.

Güvenli bir siber ortam oluşturmak için; siber ortama dâhil olan bileşenlerin koruma stratejilerinin belirlenmesi, siber saldırı durumunda gerçekleştirilecek süreçleri düzenleyen yasal mevzuatın oluşturulması, siber güvenlikle alakalı teşkilatlanmanın gerçekleştirilmesi gibi siber ortamı düzenleyen politikaların ortaya konması gerekmektedir.

Bu kapsamda ortaya konan politika ve stratejiler ele alınmış, oluşturulacak çatı üzerinde değerlendirilebilecek en önde gelen çalışmalar alt maddelerde özetlenmiştir.

2.2.1. Kritik Altyapı Siber Güvenliğini İyileştirme Çerçevesi

Amerikan Ulusal Standartlar ve Teknoloji Enstitüsü (NIST) tarafından 2013 yılında endüstri, akademi ve hükümeti kapsayan, kamu ve özel sektör kuruluşları ile çalışanlarını bir araya getiren proje ile kritik altyapılardaki siber güvenliğin iyileştirilmesine yönelik bir çerçeve [16] ortaya konmuştur. Bu çerçevenin ortaya konmasının en önemli nedeni, kritik altyapı sistemlerinin artan karmaşıklığından siber tehditlerin yararlanması ve ulusun güvenliğini, ekonomisini ve sağlığını riske atmasıdır. Siber güvenlik riskleri şirketler için de gelir – gider dengesini etkileyen, yenilik yapma ve müşteri kazanma/sürdürme becerisine zarar veren unsurlar olarak görülmektedir. Bu kapsamda NIST tarafından, kritik altyapı siber risklerinin belirlenmesi, değerlendirilmesi ve yönetilmesine yardımcı olabilecek ve bilgi güvenliği önlemleri ile kontrolleri dâhil olmak üzere öncelikli, esnek, tekrarlanabilir, performansa dayalı ve uygun maliyetli bir yaklaşım ortaya konması fikri oluşmuştur.

Çerçeve üç bölümden oluşmaktadır: çerçeve çekirdeği, uygulama katmanları ve çerçeve profilleri. Çerçeve çekirdeği, sektörler ve kritik altyapı arasında ortak olan bir dizi siber güvenlik etkinliği, sonuçları ve bilgilendirici referanslardan oluşmaktadır. Çekirdeğin öğeleri, bireysel kurumsal profiller geliştirmek için ayrıntılı rehberlik sağlamaktadır. Profillerin kullanılması yoluyla çerçeve, bir kuruluşun siber güvenlik faaliyetlerini iş / görev gereksinimleri, risk toleransları ve kaynakları ile uyumlu hale getirmesine ve önceliklendirmesine yardımcı olacaktır. Katmanlar, kuruluşların siber güvenlik risklerini yönetmeye yönelik yaklaşımlarının özelliklerini görmeleri ve anlamaları için bir mekanizma sağlamakta, siber güvenlik hedeflerine öncelik vermede ve bu hedeflere ulaşmada yardımcı olmaktadır.

Çerçeve, günümüzde etkili bir şekilde çalışan standartları, yönergeleri ve uygulamaları bir araya getirerek siber güvenliğe yönelik çoklu yaklaşımlar için ortak

bir organizasyon yapısı sağlamaktadır. Dahası, siber güvenlik için küresel olarak tanınan standartlara atıfta bulunduğu için çerçeve, diğer sektörler ve toplulukların yanı sıra kritik altyapılarda siber güvenliğin güçlendirilmesi konusunda uluslararası işbirliği için bir model görevi görebilmektedir.

2.2.2. ENISA Ulusal Siber Güvenlik Stratejileri Raporu

AB içindeki ağ ve bilgi güvenliğini en üst seviyede ve etkin bir şekilde sağlanması sorumluluğuyla 2004 yılında kurulan ENISA, sürekli değişen bir ortamda siber tehditlere yanıt verebilmek için, esnek ve dinamik siber güvenlik stratejisi oluşturmak, uluslararası işbirliği sağlamak ve siber saldırılara etkin bir şekilde hazırlanmak amacıyla bu dokümanı [17] ortaya koymuştur.

Siber güvenlik ve diğer anahtar terimlerin anlaşılması ülkeden ülkeye farklılık göstermekte, bu durum ülkeler arasında siber güvenlik stratejilerine yönelik çok farklı yaklaşımlar ortaya çıkmasına neden olmaktadır. Ülkeler arasında ortak anlayış ve yaklaşım eksikliği, ihtiyacı herkes tarafından kabul edilen uluslararası işbirliğini engellemektedir.

ENISA, AB ve AB dışı ülkelerde ulusal siber güvenlik stratejilerinin en yaygın ve yinelenen unsurlarını ve uygulamalarını belirlemeyi amaçlayan bu kılavuzu geliştirmiştir. Bu bağlamda ENISA, uygulandığında tutarlı ve bütünsel bir ulusal siber güvenlik stratejisine yol açacak bir dizi somut eylem belirlemiştir. Bu kılavuz ayrıca geliştirme ve uygulama aşamasına özel bir vurgu yaparak ulusal bir siber güvenlik stratejisi yaşam döngüsü önermektedir.

2.2.3. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı

Ülkemizdeki kritik altyapıların korunması çalışmaları incelenecek olursa, önümüzdeki yıllarda siber güvenlik çalışmalarının, gelinen durum itibariyle siber güvenlik stratejileri doğrultusunda ana temasının “kritik altyapıların korunması” olacağı değerlendirilmektedir. Bu kapsamda ülkemizde yapılan en önemli çalışmaların başında Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı, 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi ve son olarak yayımlanan 2020 – 2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı [8] gelmektedir. Strateji belgesinin 22 adet eylem

maddesi ile birlikte amacı ve kapsamı genel olarak “kritik altyapıların korunması” kavramını içermektedir.

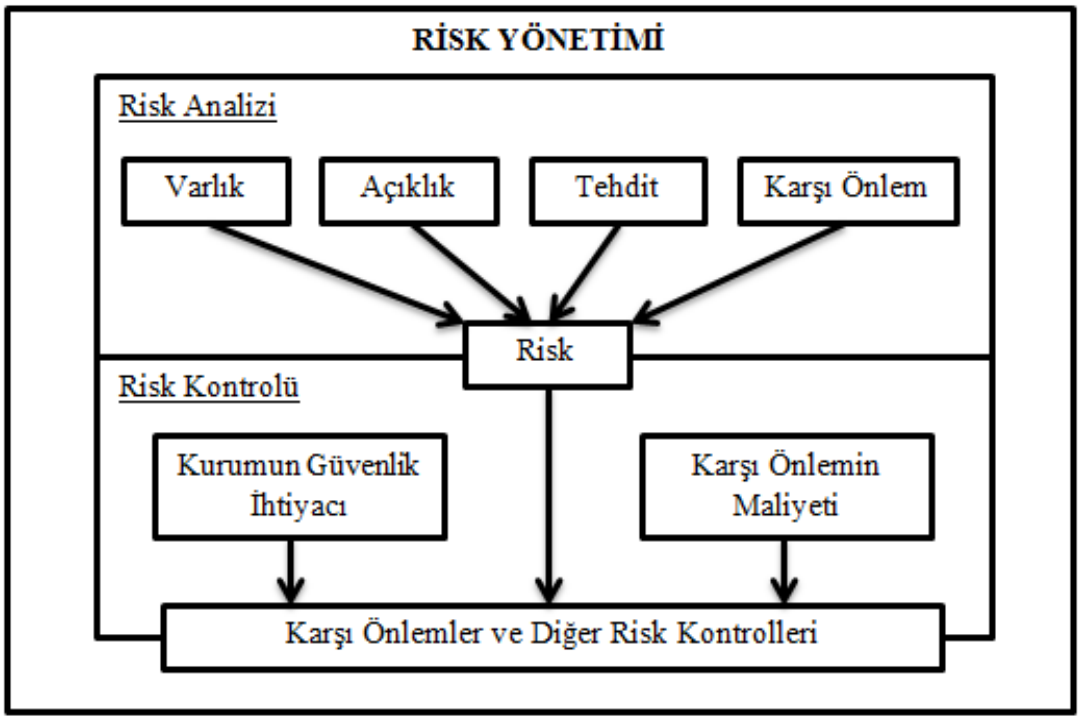
Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020- 2023), geçmiş tecrübelerden elde edilen bilgiler ışığında stratejileri daha ileriye taşımak amacıyla, siber güvenlik alanında ülkemizin belirlemiş olduğu misyon ve vizyon doğrultusunda önümüzdeki 4 yıllık döneme ait politikaları konu almaktadır. Ulusal Siber Güvenlik Stratejisi ve Eylem Planı (2020-2023), siber güvenlik seviyesini daha iyi noktalara taşımak amacıyla gerekli girişimleri sağlamak ve bu çerçevedeki faaliyetleri gerçekleştirmek amacıyla ortaya konmuştur. Bu doğrultudan hareketle bilgi ve iletişim teknolojilerindeki yenilikler ve siber güvenlik konusundaki gelişmelerin uluslararası uygulamaları da göz önüne alınarak ulusal ihtiyaçlar doğrultusunda hedefler ortaya konmuştur. Bahse konu hedefler dikkate alınarak ta ihtiyaçlar ile faaliyet planları belirlenerek çalışmaların son hali verilmiştir. Uygulamaların daha iyi düzeye getirilmesi, bilgi ve iletişim teknolojilerindeki yeniliklerden en üst seviyede faydalanılması ve insan gücünün daha etkin hale getirilmesine yönelik çalışmalar ile siber güvenlik seviyesinin artırılması amaçlanmıştır. Buradan hareketle; kritik altyapı sistemlerinin korunması amacıyla planlamalar yapılması, siber risk analizi ve yönetimi ile felaket kurtarım senaryolarının oluşturulması, yurt dışına yönelik olmayan internet trafiğinin takip edilmesi ve kontrol altına alınması ile siber güvenliğin milli güvenlik kapsamında değerlendirilmesi gibi eylemler ortaya konulmuştur.

2.3. Risk Analizi ve Yönetimi

Ulusal ve uluslar arası 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 [18][19] güvenlik politikalarının belirlenmesi ve risk yönetiminin bilgi güvenliği yönetim sisteminin ilk adımı olduğu ortaya konmuş ve bilgi güvenliği yönetiminin en önemli adımı olarak varlıklara yönelik risklerin belirlenmesi ve bu risklere karşı önlem alınması olduğu 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 – 2.3'de gösterilen risk yönetimidir.



Şekil 2.3: 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 metotlar ile sayılar kullanılır. Bu metotlar 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 uluslar arası standartlar haline dönüşmüştür. Bu kapsamda yayımlanan standartlar; ISO 31010 Risk Değerlendirme Teknikleri [20] ve ANSI 7690.3 Risk Değerlendirme Teknikleri

[21] standartlarıdır. Standartlarda belirlenen teknikler kontrol, istatistik, senaryo analizi, destek, fonksiyon analizi vb. metotlar 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 [22], COBRA [23], ISRAM [24], OCTAVE [25], RAMEX [26], TUAR [27] vb. bahse konu teknikleri kullanan birçok metodoloji geliştirilmiştir. Bu metodolojiler genel çerçevede değerlendirmeler sunmakta olup birçok farklı yapının analizinde kullanılmış [28][29] ve kıyaslamalarına yönelik çalışmalar [30] yapılmıştır. Bununla birlikte ISO 31000 Risk Yönetim Süreci Modeli [31], ISO 27005 Bilgi Güvenliği Risk Yönetim Standardı [32] ve NIST 800-39 Bilgi Güvenliği Risk Yönetim Standardı [33] gibi uluslararası standartlarda belirlenmiştir.

Yukarıda belirtilen tüm çalışmalar Risk Analiz ve Yönetiminde en kabul görmüş, birçok metodoloji/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 metodoloji/teknik/standart/model/çerçeve irdelenerek kritik altyapıların korunmasına yönelik en önemli adımlardan birine yönelik bir çerçeve tasarımı oluşturulmuştur.

2.3.1. ISO 31000 Risk Yönetimi

Bu belge [31], riskleri yöneterek, kararlar alarak, hedefler belirleyerek ve bu hedeflere ulaşarak ve performansı artırarak kuruluşlarda değer yaratan ve bunları koruyan kişilerin kullanımına yönelik olarak ortaya konmuştur. Belge ilke ve yönergeler sağlayarak, planlama, yönetim faaliyetleri ve iletişim süreçlerine uygulanabildiği kurum ve kuruluşlara risk analizleri ve risk değerlendirmelerinde yardım etmektedir. Ortaya konan süreç sayesinde, faaliyetlerdeki değişimler kontrol edilebilmekte, paydaşlarla iletişim kurulabilmekte ve riskin ele alınması için ilave hususların olup olmadığından emin olunarak mevcut riskleri değiştiren faktörler kontrol edilip, riskler izlenip, gözden geçirilebilmektedir. Risk yönetimi, bu belgede

ana hatları verilen ilkelere, çerçeveye ve sürece dayanmaktadır. Bu bileşenler önemli ölçüde risk yönetim süreçlerinin temelini oluşturmaktadır.

2.3.2. ISO 31010 Risk Değerlendirme Teknikleri

Risk yönetimi süreci, gelecekteki olayların veya şartların (kasıtlı veya kasıtsız) olasılığı ile bu olasılığın belirlenen hedefler üzerindeki etkilerini göz önüne alarak karar vermeye yardımcı olmaktadır. Risk değerlendirmesi ise, risk yönetiminin, hedeflerin nasıl etkilenebileceğini tanımlayan yapılandırılmış bir süreç sağlayan ve daha fazla tedavinin gerekip gerekmediğine karar vermeden önce sonuçlar ve olasılıkları açısından riski analiz eden bir parçasıdır.

Risk değerlendirmesi, temel olarak aşağıdaki sorularından yanıtları üzerinden yürür:

- Ne olabilir ve neden (risk belirleyerek)?
- Sonuçları nelerdir?
- Gelecekte meydana gelme olasılığı nedir?
- Riskin olasılığını veya sonuçlarını hafifleten herhangi bir husus bulunmakta mıdır? Risk düzeyi göz ardı edilebilir mi yoksa kabul edilebilir mi ve daha fazla müdahale gerektiriyor mu?

Bu standart [20], risk değerlendirme tekniklerinin belirlenmesi ve hâlihazırdaki en iyi uygulamaların ortaya konmasını amaçlamakta ve mesleki açıdan kabul edilebilir bir fikir birliği seviyesine gelmemiş yeni veya gelişen kavramlara atıfta bulunmamaktadır. Bu standart, doğası gereği geneldir, bu nedenle birçok endüstri ve sistem türü için rehberlik edebilmektedir. Bu endüstrilerde, belirli uygulamalar için tercih edilen metodolojileri ve değerlendirme seviyelerini belirleyen daha özel standartlar olabilmektedir.

2.3.3. ISO 27005 Bilgi Güvenliği Risk Yönetimi

ISO / IEC 27005 [32], kuruluşların bilgi güvenliği risk yönetimini iyileştirmesine ve iş kesintisi riskini en aza indirmesine yardımcı olmak amacıyla

geliştirilmiştir. Bir kuruluştaki bilgi güvenliği risk yönetimi için yönergeler sağlamaktadır. Ancak bu belge, bilgi güvenliği risk yönetimi için herhangi bir özel yöntem sağlamaz. Örneğin bir bilgi güvenliği yönetim sisteminin (BGYS) kapsamına, risk yönetimi bağlamına veya endüstri sektörüne bağlı olarak risk yönetimine yaklaşımlarını tanımlamak kuruluşa kalmıştır. Bir BGYS'nin gerekliliklerini uygulamak için bu belgede açıklanan çerçeve altında bir dizi mevcut metodoloji kullanılabilmektedir. Bu belge, ISO / IEC 27001 tarafından gerekli olmayan varlık, tehdit ve güvenlik açığı riski tanımlama yöntemine dayanmaktadır. Kullanılabilecek başka yaklaşımlar da mevcuttur. Bu belge, ISO / IEC 27001'de verilen BGYS gereksinimlerinin uygulanmasına ilişkin doğrudan rehberlik içermemektedir.

2.3.4. NIST 800-39 Bilgi Güvenliği Riskini Yönetme

Bu belge [33], federal hükümet için birleşik bir bilgi güvenliği çerçevesi oluşturma çabası içinde, Sivil, Savunma ve İstihbarat Topluluklarından temsilcilerle birlikte Ortak Görev Gücü Dönüşüm Girişimi Teşkilatlar Arası Çalışma Grubu tarafından geliştirilmiştir. NIST Özel Yayını 800-39, NIST tarafından geliştirilen bilgi güvenliği standartları ve yönergeleri serisinin en önemli belgesidir. Özel Yayın 800-39'un amacı, kurumsal operasyonlar (yani, görev, işlevler, imaj ve itibar), kurumsal varlıklar, bireyler, diğer kuruluşlar ve diğer kuruluşlar için bilgi güvenliği riskini yönetmek için tümleşik ve kuruluş çapında bir program için rehberlik sağlamaktır. Bu yayında sağlanan kılavuz, kuruluşların diğer mevzuat, direktifler, politikalar, programatik girişimler tarafından kapsanan risk yönetimi alanlarını ele alan diğer riskle ilgili faaliyetlerin, programların, süreçlerin veya yaklaşımların yerine geçmesi veya bunları kapsaması amaçlanmamıştır. Bunun yerine, burada açıklanan risk yönetimi kılavuzu, daha kapsamlı bir Kurumsal Risk Yönetimi programının bir parçası olarak tamamlayıcı niteliktedir ve bu çerçevede kullanılması önerilmektedir.

2.4. Konu Üzerine Yapılan 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 [34] 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 [35] 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 [36] 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 [37] 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 [38] 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 [39] 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 [40] 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 [41] 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 [42][43] 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. KRİTİK ALTYAPILARDA SİBER RİSK ANALİZİ VE YÖNETİMİNE YÖNELİK ÇERÇEVE ÖNERİSİ

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 önermektedir. 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 – 3.1'de 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 3.1: Kritik Altyapılarda Siber Risk Analizi ve Yönetimi Çerçevesi Modeli.

3.1. Önerilen Çerçeve Tasarımı

Toplam kalite yönetimindeki PUKÖ döngüsünün temelinde ISO 31000 Risk Yönetim Süreci yaklaşımının Şekil – 3.2'de yer alan tasarımı üzerine kurulacak çerçeve 5 adımdan oluşmaktadır. Bu adımlar içerisinde gerçeklenmesine 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 3.2: Kritik Altyapılarda Siber Risk Analizi ve Yönetimi Çerçevesi Modeli Adımları.

3.1.1. 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 belirlenmesindeve 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 [6] 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-3.3'de [6] genel

şablonu yer alan çekirdeğe risk değerlendirmesi aşamasında kullanılmak üzere varlık ve zafiyet sütunu eklenerek sistem verileri aktarılabilecektir.

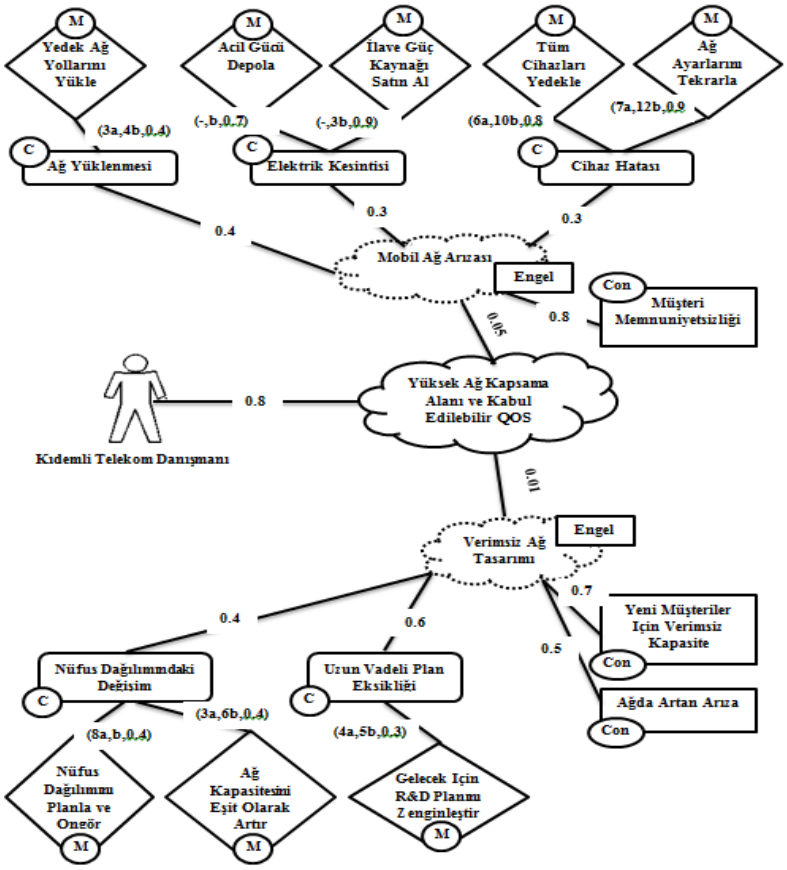
Fonksiyonlar	Kategoriler	Alt Kategoriler	Bilgilendirici Referanslar
TANIMLAMA			
KORUMA			
TESPİT			
KARŞILIK VERME			
KURTARMA			

Şekil 3.3: Sistem Gereklilikleri Şablonu.

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 – 3.4'de [34] 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 [31][32][33] 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 3.4: Senaryo Tabanlı Yaklaşım Modeli.

- 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 (3.1) ve (3.2) no'lu eşitliklerle varlık üzerindeki risk hesaplanmaktadır.

$$R_{vO} = V_{DO} * P_O * N_{PS} \tag{3.1}$$

$$R_{vM} = V_{DM} * P_M * N_{PS} \tag{3.2}$$

Tablo 3.1: Semboller Tablosu – 1.

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 [31][32][33] 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.

Tablo 3.2: Bilgi Güvenliği Değerlendirme Matrisi.

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

Varlığın bilgi güvenliği açısından önem düzeyi [19] Tablo – 3.2'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 [44] bulunmaktadır. Kabul görmüş bir çalışmanın çerçeve içerisine dâhili ile perspektif yaklaşımdan standartlaşmaya daha da yaklaşılabilecektir.

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 [45][46] da yapılmaktadır. Varlığın mali değerinin hesabında, elde etme maliyeti, işlem maliyeti ve kaybedilen iş fırsatı gibi üç öğe öne çıkmaktadır [46]. 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 (3.3) no'lu eşitlikte gösterildiği gibi toplam maliyetin temelini oluşturmaktadır.

$$F_v = \sum_{i=1}^{n} DY_i L_i + \sum_{j=1}^{m} C_j M_j + IA \tag{3.3}$$

Tablo 3.3: Semboller Tablosu – 2.

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 (3.4) ve (3.5)

no'lu ifadelerde belirtildiği şekilde etkilenen varlığın önem düzeyi ve etkilenme oranıyla ifade edilebilir.

$$D_{vO} = \sum_{i=1}^{n} V_{öi} O_{vi} * N_{PS} \,/\, n \tag{3.4}$$

$$D_{vM} = Max(V_{ö} * O_{v}) * N_{PS} \tag{3.5}$$

Varlık değerinin belirlenmesi amacıyla yukarıda belirtilen eşitliklerin parametreleri içerik oluşturma safhasında üretilmesini müteakip (3.6), (3.7) ve (3.8) no'lu eşitlikler ile varlık değerinin hesaplaması yapılabilecektir.

$$N_{PV} = Max\big(MP(G,B,E)\big) * F_K * Max(D_v) \tag{3.6}$$

$$V_{DM} = MP(G,B,E) * F_v * \; D_{vM}/N_{PV} * N_{PS} \tag{3.7}$$

$$V_{DO} = MP(G,B,E) * F_v * \; D_{vO}/N_{PV} * N_{PS} \tag{3.8}$$

Tablo 3.4: Semboller Tablosu – 3.

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)
$V_{Ö}$	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 [31][32][33] 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. Zafiyet ve Tehdit değerleri yukarıda belirtilen çerçeve ile organizasyon tarafından belirlenerek (3.9) ve (3.10) no'lu eşitlikler üzerindeki yerlerini alacaklardır.

$$P_M = Max(Z * T) * N_{PS} \tag{3.9}$$

$$P_O = \frac{\sum_{i=1}^{n} Z * T}{n} * N_{PS} \tag{3.10}$$

Tablo 3.5: Semboller Tablosu – 4.

Sembol	Tanım
Z	Zafiyet
T	Tehdit

- Sistem katmanında (3.11) ve (3.12) no'lu eşitliklerde belirtilen riskin hesaplanması senaryo tabanlı yaklaşım gereği kurulacak senaryoların hedefleri üzerinden yapılacaktır. Hedeflerin gerçekleşmemesi riski 3 temel faktöre dayanmaktadır. En önemli parametre (3.13) ve (3.14) no'lu 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.

$$R_{sO} = R_{PO} * D_{sO} * N_{PS} \tag{3.11}$$

$$R_{sM} = R_{PM} * D_{sM} * N_{PS} \tag{3.12}$$

$$R_{PO} = \left(\frac{\sum_{i=1}^{n}\left(\frac{\sum_{J=1}^{m} R_{vOj} * O_{RTi}}{m}\right)}{n} + \frac{\sum_{k=1}^{o}\left(\frac{\sum_{l=1}^{p} R_{vOl} * O_{REk}}{p}\right)}{o} + \frac{\sum_{t=1}^{r}\left(\frac{\sum_{u=1}^{s} R_{vOu} * O_{RGt}}{s}\right)}{r}\right) N_{PS}/3 \tag{3.13}$$

$$R_{PM} = Max(O_{RT}, O_{RE}, O_{RG}) * R_{vM} * N_{PS} \tag{3.14}$$

Tablo 3.6: Semboller Tablosu – 5.

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 metodolojik yöntemler kullanılarak organizasyonun yönetimi tarafından belirlenmelidir. Eşitlik (3.15) ve (3.16)'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.

$$D_{sO} = \left(\sum_{i=1}^{n} C_{Hi} \sum_{j=1}^{m} H_{\ddot{o}j} O_{Hj}\right) * N_{PS}^{2}/nm \tag{3.15}$$

$$D_{sM} = Max(C_H H_{\ddot{o}} O_H) * N_{PS}^{2} \tag{3.16}$$

Tablo 3.7: Semboller Tablosu – 6.

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

- Toplum katmanında kritik altyapı üzerindeki genel risk değerlendirmesi (3.17) ve (3.18) no'lu ifadeler ile üretilmiş olacaktır. Toplum katmanındaki risk düzeyini etkileyen temel değer hedeflerin gerçekleşme oranı ve bahse konu hedeflerin her birinin kritik altyapı için önem düzeyi olduğu görülmektedir. Buradaki yapıya etki edecek (3.19) ve (3.20) no'lu 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.

$$R_{tO} = \frac{\sum_{i=1}^{n} H_{si} H_{öi}}{n} * D_{tO} * N_{PS}^2 \tag{3.17}$$

$$R_{tM} = Max(H_s H_ö) * D_{tM} * N_{PS}^2 \tag{3.18}$$

$$D_{tO} = \frac{\sum_{i=1}^{n} K_{öi} O_{Ki}}{n} * BGYS * N_{PS}^2 \tag{3.19}$$

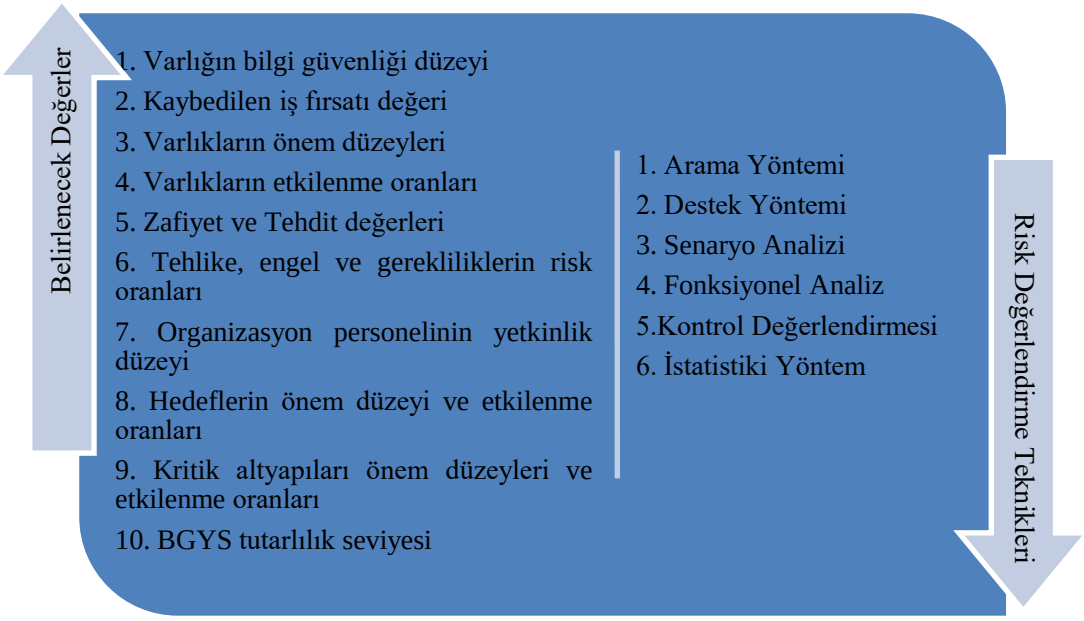
$$D_{tM} = Max(K_ö O_K) * BGYS * N_{PS}^2 \tag{3.20}$$

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.

Tablo 3.8: Semboller Tablosu – 7.

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
$H_Ö$	Hedefin önem düzeyi
$K_Ö$	Etkilenen diğer kritik altyapıların önem düzeyi
O_K	Etkilenen diğer kritik altyapıların etkilenme oranı
$BGYS$	Bilgi Güvenliği Yönetim Sisteminin tutarlılık seviyesi

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.



Şekil 3.5: Belirlenecek Değerler ve Risk Değerlendirme Teknikleri.

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 – 3.5'de belirlenmesi gereken veriler ile kullanılabilecek teknikler gösterilmiştir.

Tablo 3.9: 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

İçerik oluşturma safhasında risk yönetim organizasyonu tarafından belirlenmesine ihtiyaç duyulan değerler Tablo – 3.9'da 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 metodolojileri, araçlar ve teknikler belirlenmelidir. Bununla birlikte bu aşama ile risk yönetim sürecinin risk tanımlama ve risk değerleme maddeleri gerçeklenmiş olmaktadır.

3.1.2. Risk Değerlendirmesi

Risk değerlendirme süreci; risk belirleme, analiz ve kıyaslama olmak üzere 3 aşamadan oluşmaktadır. Risk belirleme aşaması uluslar arası 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.

3.1.3. 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 (3.21) no'lu eşitlik ile bir eşik puanı üretilerek risk yönlendirme işleminin yöneleceği süreç belirlenebilecektir.

$$E = (V_{DM} - (F_{KÖ} + IA)) * O_R \tag{3.21}$$

Tablo 3.10: Semboller Tablosu – 8.

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;

- 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 yönetim organizasyonunun bahse konu risk grubuna karşı oluşturduğu kültürde önemli olmaktadır.
- Maliyet etkin çözümler yani düşük maliyet ile yüksek risk ortadan kaldırma çözümleri sisteme derhal uygulanmasında fayda gözüken durumlar olarak göze çarpmaktadır.
- 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.
- 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.

3.1.4. 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 metodolojilerin 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.

3.1.5. 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 ÇALIŞMASI VE DEĞERLENDİRME

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.

4.1.1. İçerik Oluşturma

- 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.
- 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.
    - Örnek üzerindeki değerlendirmede genel risk puanının %1,5 ve üzeri değeri kabul edilebilir olarak görülmeyecek,
    - Bununla birlikte ağ altyapısı üzerinde de varlık bazlı risk puanı olarak %10 ve altı değerler aranacak,

- Veri tabanları üzerinde herhangi bir risk transferi işlemi uygulanmayacak,
- Risk sonlandırma amacıyla yapılacak işlemlerde bilgi güvenliği değeri 9 olan varlıklar sistemden çıkarılmayacaktır.

- Risk Protokolleri: Belirlenecek risk yönetim organizasyonunun en önemli görevlerinden birisi değerleme aşamasında organizasyon tarafından belirlenmesi gereken verilerin üretim metodolojilerinin belirlenmesidir. Burada uluslar arası standartlar üzerinden metodoloji belirlemesi yapılacağı gibi geçmiş veriler ve hâlihazırda literatürdeki standart puanlar üzerinden bir değerleme de yapılabilecektir. Bu kapsamda belirlenecek değerler için örneğimizde uygulayacağımız protokoller Şekil – 4.1'de olduğu gibidir. Birden fazla belirlenen protokolün değerlerinin aritmetik ortalaması hesaplanacaktır.

Şekil 4.1: Risk Protokolleri.

- 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.

4.1.2. 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;

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

$$N_{PV} = Max\big(MP(G,B,E)\big) * F_K * Max(D_v) \tag{4.1}$$

$$N_{PV} = 9 * 100 * 90 = 81000 \tag{4.2}$$

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

$$D_{vO} = \sum_{i=1}^{n} V_{öi} O_{vi} * N_{PS} \,/\, n \tag{4.3}$$

$$\begin{aligned} D_{vO} &= \big((90 * 70) + (95 * 80) + \cdots..\big) * 0{,}01/n \\ &= 80\ (Ağ\ Altyapısı) \end{aligned} \tag{4.4}$$

$$\begin{aligned} D_{vO} &= \big((80 * 75) + (90 * 60) + \cdots..\big) * 0{,}01/n \\ &= 70\ (Veri\ Tabanları) \end{aligned} \tag{4.5}$$

$$\begin{aligned} D_{vO} &= \big((85 * 70) + (90 * 75) + \cdots..\big) * 0{,}01/n \\ &= 75\ (Disk\ Üniteleri) \end{aligned} \tag{4.6}$$

$$V_{DO} = MP(G, B, E) * F_v * \ D_{vO}/N_{PV} * N_{PS} \tag{4.7}$$

$$V_{DO} = 8 * 40 * \ 80/81000 * 0{,}01 = 31{,}6(Ağ\ Altyapısı) \tag{4.8}$$

$$V_{DO} = 8 * 38 * \ 70/81000 * 0{,}01 = 26{,}27(Veri\ Tabanları) \tag{4.9}$$

$$V_{DO} = 9 * 35 * \ 75/81000 * 0{,}01 = 29{,}16(Disk\ Üniteleri) \tag{4.10}$$

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

$$P_O = \frac{\sum_{i=1}^{n} Z * T}{n} * N_{PS} \tag{4.11}$$

$$P_O = \frac{(10 * 90) + (40 * 70) + \cdots \ldots}{n} * 0{,}01 = 40(Ağ\ Altyapısı) \tag{4.12}$$

$$P_O = \frac{(30 * 70) + (15 * 85) + \cdots \ldots}{n} * 0{,}01 = 35(Veri\ Tabanları) \tag{4.13}$$

$$P_O = \frac{(20 * 95) + (30 * 80) + \cdots \ldots}{n} * 0{,}01 = 70(Disk\ Üniteleri) \tag{4.14}$$

$$R_{vO} = V_{DO} * P_O * N_{PS} \tag{4.15}$$

$$R_{vO} = 31{,}6 * 40 * 0{,}01 = 12{,}64(Ağ\ Altyapısı) \tag{4.16}$$

$$R_{vO} = 26{,}27 * 35 * 0{,}01 = 9{,}19(Veri\ Tabanları) \tag{4.17}$$

$$R_{vO} = 29{,}16 * 70 * 0{,}01 = 20{,}41(Disk\ Üniteleri) \tag{4.18}$$

- 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 hesaplanır.

$$R_{PO} = \left(\frac{\sum_{i=1}^{n}\left(\frac{\sum_{J=1}^{m} R_{vOj} * O_{RTi}}{m}\right)}{n} + \frac{\sum_{k=1}^{o}\left(\frac{\sum_{l=1}^{p} R_{vOl} * O_{REk}}{p}\right)}{o} + \frac{\sum_{t=1}^{r}\left(\frac{\sum_{u=1}^{s} R_{vOu} * O_{RGt}}{s}\right)}{r}\right) N_{PS}/3 \tag{4.19}$$

$$R_{PO} = \left(\left(\frac{(10{,}8 + 7{,}6 + \cdots)70 + (9{,}6 + 12{,}5 + \cdots)80 + \cdots}{mn}\right) + \left(\frac{(9{,}4 + 8{,}6 + \cdots)75 + (10{,}6 + 12{,}5 + \cdots)60 + \cdots}{po}\right) + \left(\frac{(6{,}8 + 7{,}7 + \cdots)60 + (10{,}8 + 11{,}5 + \cdots)90 + \cdots}{sr}\right)\right)0{,}01/3 = 7{,}14(Hedef - 1) \quad (4.20)$$

$$R_{PO} = \left(\left(\frac{(11{,}6 + 8{,}4 + \cdots)80 + (8{,}6 + 9{,}8 + \cdots)90 + \cdots}{mn}\right) + \left(\frac{(8{,}4 + 11{,}6 + \cdots)85 + (11{,}6 + 8{,}3 + \cdots)70 + \cdots}{po}\right) + \left(\frac{(8{,}8 + 8{,}7 + \cdots)90 + (10{,}7 + 9{,}4 + \cdots)85 + \cdots}{sr}\right)\right)0{,}01/3 = 8{,}88(Hedef - 2) \quad (4.21)$$

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.

$$D_{sO} = (\sum_{i=1}^{n} C_{Hi} \sum_{j=1}^{m} H_{öj} O_{Hj}) * N_{PS}^2/nm \quad (4.22)$$

$$D_{sO} = \left((40 + 50 + \cdots.)\left((70 * 80) + (85 * 90) + ..\right)\right) * \frac{0{,}01^2}{nm} = 35(Hedef - 1) \quad (4.23)$$

$$D_{sO} = \Big((60 + 55 + \cdots.)\big((80 * 60) + (95 * 70) + ..\big)\Big) * \frac{0{,}01^2}{nm} = 37(Hedef - 2) \tag{4.24}$$

$$R_{sO} = R_{PO} * D_{sO} * N_{PS} \tag{4.25}$$

$$R_{sO} = 7{,}14 * 35 * 0{,}01 = 2{,}499(Hedef - 1) \tag{4.26}$$

$$R_{sO} = 8{,}88 * 37 * 0{,}01 = 3{,}2856(Hedef - 2) \tag{4.27}$$

- 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.

$$D_{tO} = \frac{\sum_{i=1}^{n} K_{öi} O_{Ki}}{n} * BGYS * N_{PS}^2 \tag{4.28}$$

$$D_{tO} = \frac{(70 * 80) + (90 * 90) + \cdots \ldots}{n} * 80 * 0{,}01^2 = 60 \tag{4.29}$$

$$R_{tO} = \frac{\sum_{i=1}^{n} H_{si} H_{öi}}{n} * D_{tO} * N_{PS}^2 \tag{4.30}$$

$$R_{tO} = \frac{(2{,}4 * 80) + (3{,}2 * 90) + \cdots \ldots.}{n} * 60 * 0{,}01^2 = \mathbf{1,53} \tag{4.31}$$

4.1.3. 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;

- Riskin tedavisi varlık bazlı olarak kabul görse bile genel ve ağ altyapısı bazında tedavi edilmeyeceği belirlenmiştir. Bu nedenle genel riski azaltmak adına varlık bazlı ağ altyapısı haricinde de işlemler gerekebilecektir.
- 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.

$$E = (V_{DM} - (F_{KÖ} + IA)) * O_R \tag{4.32}$$

$$E = \big(35 - (10 + 6)\big) * 75 = 1425 \tag{4.33}$$

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.

- 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;

$$E = (V_{DM} - (F_{KÖ} + IA)) * O_R \tag{4.34}$$

$$E = \big(35 - (9 + 4)\big) * 60 = 1320 \tag{4.35}$$

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.

- 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.

4.1.4. 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 kararlı 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.

4.1.5. 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.

4.2.1. 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.

Tablo 4.1: Kıyaslama Tablosu.

Yöntem / Özellik	Tasarlanan Çalışma	Bagheri ve Ghorbani'nin Yöntemi [34]	Romanowski ve Schneider'in Yöntemi [35]	Chen'in Yöntemi [36]	Avrupa Komisyonu Çalışması [37]	Kumaş ve Birgören'in Yöntemi [38]	Feglar ve Levy'nin Yöntemi [39]	Heo'nin Yöntemi [40]
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(değerleme 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	Sınırlı	Sınırlı	Sınırlı

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 Tablo – 4.1 üzerinde değerlendirme yapılabilecektir.

4.2.2. 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, ÖNERİLER VE GELECEK ÇALIŞMASI

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 uluslar arası 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.

KAYNAKLAR

[1] Web 1, (2019), Microsoft Global Cyber Risk Perception Survey, https://www.marsh.com/us/insights/research/marsh-microsoft-cyber-survey-report-2019.html, (Erişim Tarihi: 30/04/2021).

[2] Web 2, (2019), Kaspersky Security Bulletin Statistics, https://securelist.com/kaspersky-security-bulletin-2019-statistics/95475/, (Erişim Tarihi: 30/04/2021).

[3] Web 3, (2019), Symantec Internet Security Threat Report Volume 24, https://docs.broadcom.com/doc/istr-24-2019-en, (Erişim Tarihi: 30/04/2021).

[4] Web 4, (2021), The Official World Wide Web Anniversary Site, https://www.internetlivestats.com, (Erişim Tarihi: 30/04/2021).

[5] Web 5, (2019), Kaspersky A Global Survey into Attitudes and Opinions on IT Security, https://media.kaspersky.com/documents/business/brfwn/en/The-Kaspersky-Lab-Global-IT-Risk-Report_Kaspersky-Endpoint-Security-report.pdf, (Erişim Tarihi: 30/04/2021).

[6] E. Byres and J. Lowe, (2004), The myths and facts behind cyber security risks for industrial control systems, presented at the VDE Congress, Garmisch-Partenkirchen, Germany, 3-4 May 2004.

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

[8] UDHB, (2019), 2020 – 2023 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, Ulaştırma Denizcilik ve Haberleşme Bakanlığı.

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

[10] BTK, (2011), BTK Kritik Altyapıların Korunması Belgesi, Bilgi Teknolojileri ve İletişim Kurumu.

[11] USDHS, (2006), National Infrastructure Protection Plan, United States Department of Homeland Security.

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

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

[14] Jung-Ho E., Nam-Uk K., Sung-Hwan K., Tai-Myoung C., (2012), "Cyber Military Strategy for Cyberspace Superiority in Cyber Warfare", 2012 International Conference on Cyber Security, Cyber Warfare and Digital Forensic, 295-298, Kuala Lumpur, Malaysia, 26-28 June 2012.

[15] OECD, (2008), Working Party on Information Security and Privacy, "Recommendations of the Council on the Protection of Critical Information Infrastructures", January 2008.

[16] NIST, (2018), Framework for Improving Critical Infrastructure Cyber Security, National Institute of Standards and Technology.

[17] ENISA, (2012), National Cyber Security Strategies, Practical Guide on Development and Execution, The European Union Agency for Cybersecurity, December 2012.

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

[19] ISO, (2005), 27001 Information Security Management System, International Organization for Standardization.

[20] ISO, (2009), 31010 Risk Assessment Techniques, International Organization for Standardization.

[21] ANSI, (2011), Z690.3 Risk Assessment Techniques, American National Standards Institute.

[22] Security Service on behalf of the UK Government, (1996), "CRAMM Management Guide", first published April 1996.

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

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

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

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

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

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

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

[30] Sarkheyli A., Ithnin N.B., (2010), “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.

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

[32] ISO, (2011), 27005 Information Security Risk Management, International Organization for Standardization.

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

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

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

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

[37] 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.

[38] Kumaş E., Birgören B., (2010), “E-Devlet Kapısı Projesi Bilgi Güvenliği ve Risk Yönetimi: Türkiye Uygulaması”, Bilişim Teknolojileri Dergisi, 3(2), 29-36, Mayıs 2010.

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

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

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

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

[43] Guzman A., Ishida S., Choi E., Aoyama A., (2016), “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.

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

[45] Hua J., Bapna S., (2012), “The Economic Impact of Cyber Terrorism”, Elsevier The Journal of Strategic Information Systems, 22(2), 175-186, June 2013.

[46] Park W.H., (2012), “Risk Analysis and Damage Assessment of Financial Institutions in Cyber Attacks between Nations”, Elsevier Mathematical and Computer Modelling, 58(11-12), 1845, December 2013.

ÖZGEÇMİŞ

Emre KIRAN ilk ve ortaöğrenimi ülkemizin çeşitli şehirlerinde tamamlamasını müteakip 2004 yılında başladığı Karadeniz Teknik Üniversitesi Mühendislik Mimarlık Fakültesi Bilgisayar Mühendisliği Bölümünü 2009 yılında başarıyla tamamladı. Yüksek lisans eğitimine 2019 yılında Gebze Teknik Üniversitesi Fen Bilimleri Enstitüsü Bilgisayar Mühendisliği Anabilim Dalında başladı. 2011 yılından bu yana bir kamu kurumunda bilgi sistemleri işletme/yönetim alanında çalışmaktadır.

EKLER

Ek A: Tez Çalışması Kapsamında Yapılan Yayınlar

Soğukpınar İ., Kıran E., "Kritik Altyapılarda Siber Risk Analizi ve Yönetimi", Türkiye Bilişim Vakfı Bilgisayar Bilimleri ve Mühendisliği Dergisi, Cilt:14 – Sayı:1, 2021.

Ek B: Örnek Varlık – Zafiyet Eşleştirme Tablosu

Fonksiyonlar	Kategoriler	Alt Kategoriler	Varlık	Zafiyet	Kaynak
Tanımlama	Varlık Yönetimi	Organizasyon haberleşme ve veri akış haritasının oluşturulması	Ağ altyapısı	Korunmasız iletişim hatları	• CCS CSC 1 • COBIT 5 DSS05.02 • ISA 62443-2-1:2009 4.2.3.4 • ISO/IEC 27001:2013 A.13.2.1 • NIST SP 800-53 Rev.4 AC-4, CA-3, CA-9 PL-8
			Ağ Cihazları	Periyodik yerleşim şeması eksikliği	
		Yazılım platformları ve uygulamalarının envantere edilmesi	Uygulama yazılımları	Yazılımların yetersiz test edilmesi veya hiç test edilmemesi	• CCS CSC 2 • COBIT 5 BAI09.01, BAI09.02, BAI09.05 • ISA 62443-2-1:2009 4.2.3.4 • ISA 62443-3-3:2013 SR 7.8 • ISO/IEC 27001:2013 A.8.1.1, A.8.1.2 • NIST SP 800-53 Rev.4 CM-8
			Uygulama yazılımları	Yaygın olarak dağıtılmış yazılım	
	Yönetim	Organizasyonun bilgi güvenliği politikalarının yayımlanması	SOME	Değişim kontrol prosedürleri eksikliği	• COBIT 5 APO01.03, EDM01.01, EDM01.02 • ISA 62443-2-1:2009 4.3.2.6 • ISO/IEC 27001:2013 A.5.1.1 • NIST SP 800-53 Rev.4 -1 controls from all families
			Güvenlik cihazları	Erkin konfigürasyon değişimi ihlali	
		Bilgi güvenliği rolleri ve sorumluluklarının koordinesi ve iç roller ile dış partnerlerin düzenlenmesi	SOME	Yazılım ve donanımın hatalı kullanımı	• COBIT 5 APO13.12 • ISA 62443-2-1:2009 4.3.2.3.3 • ISO/IEC 27001:2013 A.6.1.1, A.7.2.1 • NIST SP 800-53 Rev.4 PM-1, PS-7
			Güvenlik cihazları	Elektromanyetik radyasyona duyarlılık	
Koruma	Erişim Kontrolü	Uzaktan erişim yönetimi	Veri tabanları	Yetkisiz erişim	• COBIT 5 APO13.01, DSS01.04, DSS05.03 • ISA 62443-2-1:2009 4.3.3.6.6 • ISA 62443-3-3:2013 SR 1.13, SR 2.6
			Sunucular	İş istasyonundan çıkılınca logout olmama	

					• ISO/IEC 27001:2013 A.6.2.2, A.13.1.1, A.13.2.1 • NIST SP 800-53 Rev.4 AC-17, AC-19, AC-20
		Varlıklara fiziki erişim yönetimi ve koruması	Sunucular	Binalara ve odalara fiziksel erişim kontrolünün yetersiz ve dikkatsiz yapılması	• COBIT 5 DSS01.04, DSS05.05 • ISA 62443-2-1:2009 4.3.3.3.2, 4.3.3.3.8 • ISA 62443-3-3:2013 A.11.1.1, A.11.1.2, A.11.1.4, A.11.1.6, A.11.2.3 • NIST SP 800-53 Rev.4 PE-2, PE-3, PE-4, PE-5, PE-6, PE-9
			Disk üniteleri	Binalara ve odalara fiziksel erişim kontrolünün yetersiz ve dikkatsiz yapılması	
	Veri Güvenliği	Saklanan verilerin korunması	Disk üniteleri	Kontrolsüz kopyalama	• CCS CSC 17 • COBIT 5 APO01.06, BAI02.01, BAI06.01, DSS06.06 • ISA 62443-3-3:2013 SR 3.4, SR 4.1 • ISO/IEC 27001:2013 A.8.2.3 • NIST SP 800-53 Rev.4 SC-28
			Yedekleme birimleri	Kontrolsüz depolama	
		İletilen verilerin korunması	Ağ altyapısı	Haberleşme hatlarının korunmaması	• CCS CSC 17 • COBIT 5 APO01.06, DSS06.06 • ISA 62443-3-3:2013 SR 3.1, SR 3.8, SR 4.1, SR 4.2 • ISO/IEC 27001:2013 A.8.2.3, A.13.1.1, A.13.2.1, A.13.2.3, A.14.1.2, A.14.1.3 • NIST SP 800-53 Rev.4 SC-8
			Ağ cihazları	Şifrelerin açık transfer edilmesi	
Tespit	Sürekli Güvenlik Takibi	Açıklık taraması yapılması	Ağ altyapısı	Korunmasız iletişim hatları	• COBIT 5 BAI03.10

			İşletim Sistemleri	Erişim haklarının hatalı tahsisi	• ISA 62443-2-1:2009 4.2.3.1, 4.2.3.7 • ISO/IEC 27001:2013 A.12.6.1 • NIST SP 800-53 Rev.4 RA-5
		Potansiyel siber güvenlik olaylarına karşı ağın takip edilmesi	Ağ cihazları	Gönderilen ve alınan mesajların yavaşlaması	• COBIT 5 APO07.06 • ISO/IEC 27001:2013 A.14.2.7, A.15.2.1 • NIST SP 800-53 Rev.4 CA-7, PS-7, SA-4, SA-9, SI-4
			Ağ altyapısı	Yerel alan ağının korunmaması	
	Tespit işlemleri	Tespit işlemlerini test etme	Güvenlik cihazları	Görüntüleme mekanizmaları eksikliği	• COBIT 5 APO13.02 • ISA 62443-2-1:2009 4.4.3.2 • ISA 62443-3-3:2013 SR 3.3 • ISO/IEC 27001:2013 A.14.2.8 • NIST SP 800-53 Rev.4 CA-2, CA-7, PE-3, PM-14, SI-3, SI-4
			Ağ altyapısı	Tek nokta hataları	
		Tespit bilgilerinin uygun birimlerle paylaşılması	İşletim sistemleri	Zayıf şifre yönetimi	• COBIT 5 APO12.06 • ISA 62443-2-1:2009 4.3.4.5.9 • ISA 62443-3-3:2013 SR 6.1 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev.4 CA-2, CA-7, PL-2, RA-5, SI-4, PM-14
			Uygulama yazılımları	Etkin değişim kontrolü eksikliği	
Karşı Önlem	Haberleşmeler	Olayların belirlenen kriterlere göre raporlanması	Veri tabanları	DB adminlerinin gerçekleştirdiği işlemlerin loglanmaması	• ISA 62443-2-1:2009 4.3.4.5.5 • ISO/IEC 27001:2013 A.16.1.2 • NIST SP 800-53 Rev.4 AU-6, IR-6, IR-8
			Yedekleme birimleri	Yedekleme kopyaları eksikliği	
		Bir müdahale gerektiğinde personelin rollerini ve operasyon sırasını bilmemesi	Sunucular	Yazılım ve donanımların hatalı kullanımı	• ISA 62443-2-1:2009 4.3.4.5.2, 4.3.4.5.3, 4.3.4.5.4 • ISO/IEC 27001:2013 A.6.1.1, A.16.1.1 • NIST SP 800-53 Rev.4 CP-2, CP-3, IR-3, IR-8
			Uygulama yazılımları	Hatalı parametre girişi	

	Analiz	Olayın etkisinin anlaşılması	Disk üniteleri	Depolama ortamlarının yetersiz bakımı/hatalı kurulumu	• ISA 62443-2-1:2009 4.3.4.5.6, 4.3.4.5.7, 4.3.4.5.8 • ISO/IEC 27001:2013 A.16.1.6 • NIST SP 800-53 Rev.4 CP-2, IR-4
			Güvenlik cihazları	Hassas trafiğin korunmaması	
		Olayların müdahale planları ile tutarlı olacak şekilde kategorize edilmesi	SOME	Etkisiz güvenlik eğitimleri	• ISA 62443-2-1:2009 4.3.4.5.6 • ISO/IEC 27001:2013 A.16.1.4 • NIST SP 800-53 Rev.4 CP-2, IR-4, IR-5, IR-8
			Güvenlik cihazları	Gereksiz servis kullanımı	
Kurtarma	Geliştirme	Kurtarma stratejilerinin güncel tutulması	Veri tabanları	Veri tabanı yedeklerinin olmaması	• COBIT 5 BAI07.08 • NIST SP 800-53 Rev.4 CP-2, IR-4, IR-8
			Yedekleme birimleri	Devamlılık planları yetersizliği	
		Kurtarma planlarının alınan dersleri içermesi	Disk üniteleri	Yönetici ve operatör loglarında kaydedilen hata raporlarının olmaması	• COBIT 5 BAI05.07 • ISA 62443-2-1:2009 4.4.3.4 • NIST SP 800-53 Rev.4 CP-2, IR-4, IR-8
			Yedekleme birimleri	Yönetici ve operatör loglarının kaydedilmemesi	
	Haberleşme	Yerel hakların yönetilmesi	İşletim sistemleri	Erişim hakkı inceleme için resmi süreç eksikliği	• COBIT 5 EDM03.02
			Sunucular	Düzenli yönetim yorumları eksikliği	
		Kurtarma faaliyetlerinin iç paydaşlar, yöneticiler ve yönetici ekipleriyle paylaşılması	Yedekleme birimleri	Yazılım ve donanımın hatalı kullanımı	• NIST SP 800-53 Rev.4 CP-2, IR-4
			Ağ altyapısı	Gönderilen ve alınan mesajların yavaşlaması	

Ek C: Örnek Varlık – Zafiyet – Tehdit – Risk Eşleştirme Tablosu

Varlık	Zafiyet	ISO 27005 İlişkili Tehdit	Risk
Veri tabanları	Yetkisiz erişim	Hakların kötüye kullanılması	Veri tabanları üzerindeki hakların kötüye kullanılması riski
	DB adminlerinin gerçekleştirdiği işlemlerin loglanmaması	Hakların kötüye kullanılması	Veri tabanları üzerindeki hakların kötüye kullanılması riski
	Veri tabanı yedeklerinin olmaması	Hizmet kesintisi yaşanması	Veri tabanlarında hizmet kesintisi yaşanması riski
Ağ Altyapısı	Korunmasız iletişim hatları	Telekulak	Kurum verilerinin dışarıya sızma riski
	Haberleşme hatlarının korunmaması	Telekulak	Kurum verilerinin dışarıya sızma riski
	Yerel alan ağının korunmaması	Ekipmanların yetkisiz kullanımı	Ağ altyapısının devre dışı kalması riski
	Tek nokta hatası	Haberleşme ekipmanları hatası	Ağ altyapısının devre dışı kalması riski
	Gönderilen ve alınan mesajların yavaşlaması	Eylemlerin reddi/durması	Önemli haberleşmelerin durması riski
Ağ cihazları	Periyodik yerleşim şeması eksikliği	Ekipman ya da medyanın imhası	Ağ altyapısının lokal veya genel olarak devre dışı kalması riski
	Şifrelerin açık transfer edilmesi	Uzaktan casusluk	Önemli donanımların ele geçirilmesi riski
	Gönderilen ve alınan mesajların yavaşlaması	Eylemlerin reddi/durması	Önemli haberleşmelerin durması riski
Uygulama yazılımları	Yazılımın yetersiz test edilmesi veya hiç test edilmemesi	Hakların kötüye kullanılması	Uygulama yazılımları üzerinde hakların kötüye kullanılması riski
	Yaygın olarak dağıtılmış yazılım	Veri bozulması	Uygulama verilerinin zarar görmesi riski
	Etkin değişim kontrolü eksikliği	Yazılım hataları	Uygulama yazılımlarının kullanılamaz duruma gelmesi riski
	Hatalı parametre girişi	Kullanım hataları	Uygulama yazılımlarının kullanılamaz duruma gelmesi riski
SOME	Değişim kontrol prosedürleri eksikliği	Bilgi sistem sürekliliği ihlali	Ağ altyapısının lokal veya genel olarak devre dışı kalması riski
	Yazılım ve donanımın hatalı kullanımı	Kullanım hataları	Güvenlik sistemlerinin görev yapamaz hale gelmesi riski
	Etkisiz güvenlik eğitimleri	Kullanım hataları	Güvenlik sistemlerinin görev yapamaz hale gelmesi riski
Güvenlik cihazları	Etkin konfigürasyon değişimi ihlali	Kullanım hataları	Güvenlik sistemlerinin görev yapamaz hale gelmesi riski
	Elektromanyetik radyasyona duyarlılık	Elektromanyetik radyasyon	Sistem üzerindeki verilerin dışarıya sızması riski
	Görüntüleme mekanizması eksikliği	Verileri gayri yasal işleme	Güvenlik sistemlerinin etkin çalışamaması riski
	Hassas trafiğin korunmaması	Telekulak	Kurum verilerinin dışarıya sızma riski
	Gereksiz servis kullanımı	Verilerin gayri yasal işlenmesi	Güvenlik sistemlerinin etkin çalışamaması riski
Sunucular	İş istasyonundan çıkınca logout olmama	Hakların kötüye kullanılmaması	Sunucular üzerinde hakların kötüye kullanılması riski
	Binalara ve odalara fiziksel erişim kontrolünün yetersiz ve dikkatsiz yapılması	Ekipman veya medyaların zarar görmesi	Sunucu sistemlerinin ve verilerin zarar görmesi riski
	Yazılım ve donanımın hatalı kullanımı	Kullanım hataları	Sunucuların görev yapamaz hale gelmesi riski
	Düzenli yönetim yorumları eksikliği	Ekipmanların yetkisiz kullanımı	Sunucuların yetkisiz kişiler tarafından kullanılması riski
Disk Üniteleri	Binalara ve odalara fiziksel erişim kontrolünün yetersiz ve dikkatsiz yapılması	Ekipman veya medyaların zarar görmesi	Disk ünitelerinin ve verilerin zarar görmesi riski
	Kontrolsüz kopyalama	Medya ve dokümanların çalınması	Kurum verilerinin yetkisiz kişilerin eline geçme riski
	Depolama ortamlarının yetersiz bakımı/hatalı kurulumu	Bilgi sistem sürekliliği ihlali	Üretilen verilerde kayıplar yaşanması riski

	Yönetici ve operatör loglarında kaydedilen hata raporlarının olmaması	Hakların kötüye kullanılması	Disk üniteleri üzerinde hakların kötüye kullanılması riski
Yedekleme birimleri	Kontrolsüz depolama	Medya ve dokümanların çalınması	Kurum verilerinin dışarıya sızma riski
	Yedekleme kopyaları eksikliği	Verilerin bozulması	Kurum verilerinin zarar görmesi riski
	Devamlılık planları yetersizliği	Ekipman hataları	Yedekleme birimleri ve kurum verilerinin zarar görmesi riski
	Yönetici ve operatör loglarının kaydedilmemesi	Kullanım hataları	Yedekleme birimleri ve kurum verilerinin zarar görmesi riski
	Yazılım ve donanımın hatalı kullanımı	Kullanım hataları	Yedekleme birimleri ve kurum verilerinin zarar görmesi riski
İşletim sistemleri	Erişim haklarının hatalı tahsisi	Hakların kötüye kullanılması	İşletim sistemleri üzerinde hakların kötüye kullanılması riski
	Zayıf şifre yönetimi	Hakların kaybedilmesi	İşletim sistemleri üzerinde hakların yetkisiz kişilerin eline geçmesi riski
	Erişim hakkı inceleme için resmi süreç eksikliği	Hakların kötüye kullanılması	İşletim sistemleri üzerinde hakların kötüye kullanılması riski

Ek Ç: Örnek Hedef – Risk Eşleştirme Tablosu

Hedefler	Hedefleri Etkileyen Faktörler		Varlık Katmanı ile İlişkili Riskler
	Ana Başlık	**Alt Başlık**	
Kesintisiz Elektrik Sağlamak	Gereklilikler	Sistem Bakımının Düzenli ve Zamanında Yapılması	Kurum verilerinin zarar görmesi
			Önemli haberleşmelerin durması
		İhtiyaç Analizi Yapmak	Yedekleme birimleri ve kurum verilerinin zarar görmesi
			Sunucuların görev yapamaz hale gelmesi
	Engeller	Etkisiz Ağ Tasarımı	Bilgi sistemlerinin doygunluğu
			Ağ altyapısının devre dışı kalması
		Ağın Devre Dışı Kalması	Bilgi sistemlerinin doygunluğu
			Önemli haberleşmelerin durması
	Tehlikeler	Dış Kaynaklı Saldırı	Veri tabanı üzerindeki hakların kötüye kullanılması
			Kurum verilerinin dışarıya sızması
		Bilinçsiz Kullanıcılar	Kulanım sırasında hata oluşması
			Ekipmanın ya da medyanın hasar görmesi
Kaçak Oranını En Aza İndirmek	Gereklilikler	Kontrol yazılımlarının tutarlı çalışması	Uygulama yazılımları üzerinde hakların kötüye kullanılması
			Uygulama yazılımlarının kullanılamaz duruma gelmesi
		Etkin veri analizi yapmak	Yedekleme birimleri ve kurum verilerinin zarar görmesi
			Yedekleme birimleri ve kurum verilerinin zarar görmesi
	Engeller	Düzenli bakım/tutum eksikliği	Kurum verilerinin zarar görmesi
			Sunucuların görev yapamaz hale gelmesi
		Çağın gerisinde kalmış altyapı	Düzenli veri akışı gelmemesi
			Veri kayıpları yaşanması
	Tehlikeler	Karmaşık Sistemler	Güvenlik sistemlerinin görev yapamaz hale gelmesi
			İşletim sistemleri üzerinde hakların kötüye kullanılması
		Yetkisiz kullanım	Disk ünitelerinin ve verilerin zarar görmesi
			Sunucuların görev yapamaz hale gelmesi
Elektrik Dalgalanmalarının Önüne Geçmek	Gereklilikler	Düzenli veri akışı sağlanması	Ağ altyapısının lokal veya genel olarak devre dışı kalması
			Önemli haberleşmelerin durması
		Yetkin personel kullanımı	İşletim sistemleri üzerinde hakların yetkisiz kişilerin eline geçmesi
			Sunucuların yetkisiz kişiler tarafından kullanılması
	Engeller	Kontrol eksikliği	Güvenlik sistemlerinin etkin çalışamaması
			Önemli haberleşmelerin durması
		Haberleşme sorunları yaşanması	Ağ altyapısının devre dışı kalması
			Veri tabanlarında hizmet kesintisi yaşanması
	Tehlikeler	Dış Kaynaklı Saldırı	Veri tabanı üzerindeki hakların kötüye kullanılması
			Kurum verilerinin dışarıya sızması
		Sistemin devre dışı kalması	Sunucu sistemlerinin ve verilerin zarar görmesi
			Önemli haberleşmelerin durması
Elektrik Üretimini İhtiyaçlar Oranında Artırmak	Gereklilikler	İhtiyaç Analizi Yapmak	Yedekleme birimleri ve kurum verilerinin zarar görmesi
			Sunucuların görev yapamaz hale gelmesi
		Uygulama yazılımlarının tutarlı çalışması	Uygulama yazılımları üzerinde hakların kötüye kullanılması
			Uygulama verilerinin zarar görmesi
	Engeller	Düzenli planlamalar yapılmaması	Kurum verilerinin zarar görmesi
			Üretilen verilerde kayıplar yaşanması

		Değişen sistemlerin takip edilmemesi	Uygulama yazılımlarının kullanılamaz duruma gelmesi
			Ağ altyapısının lokal veya genel olarak devre dışı kalması
	Tehlikeler	Veri kayıpları	Kurum verilerinin yetkisiz kişilerin eline geçmesi
			Yedekleme birimleri ve kurum verilerinin zarar görmesi
		Altyapının zarar görmesi	Ağ altyapısının lokal veya genel olarak devre dışı kalması
			Önemli haberleşmelerin durması

Ek D: Örnek Kritik Altyapı İlişkilendirme Tablosu

Kritik Altyapıdaki Sistem Hedefleri	**Hedeflerden Etkilenen Diğer Altyapı/Sistemler**
Kesintisiz Elektrik Sağlamak	Organize Sanayi Bölgeleri
	Sağlık Kuruluşları
	Haberleşme Altyapısı
Kaçak Oranını En Aza İndirmek	Elektrik Dağıtım Altyapısı
	Diğer Enerji Üretim Sistemleri
Elektrik Dalgalanmalarının Önüne Geçmek	Veri Merkezleri
	Haberleşme Altyapısı
Elektrik Üretimini İhtiyaçlar Oranında Artırmak	Şehir Şebekesi
	Organize Sanayi Bölgeleri