	Bu bölüm BAPK tarafından			
Proje Numarası	BGYS	2	7	1

1. Proje Başlığı		
ISO 27001 BGYS Doküman ve Belgelendirme Süreci		
2. Önerilen Proje Süresi (ay)	**3. Toplam Bütçe (TL)**	**4. İstenen destek miktarı (TL)**
12 AY	1,380,599 TL	300,000 TL
5. Proje ile ilgili olarak başka bir kurumdan destek istendi mi? İstendi ise Hangi kurumdan?		
Enderun Akademi ve Kurumsal Çöz. Hiz. Ltd. Şti. – Danışman Kuruluş KİWA Belgelendirme Hizmetleri A.Ş. - Belgelendirme Kuruluşu Nebula Bilişim Sistemleri Sanayi ve Ticaret Ltd. Şti. - Penetrasyon Testi (Sızma), DLP için Veri Sınıflandırma ve Varlık Tespiti Danışmanlık Hizmeti, Spam ve Phishing Farkındalık Eğitimi		
6. Proje dokümanındaki bir kısmı ya da tamamı kullanılarak başka bir destek programına başvuru yapıldı mı? Yapıldı ise yılı ve destek programının adı nedir? (BAP, DPT, TÜBİTAK, SANTEZ vb)?		
2024 yılında KOSGEB Belgelendirme Desteği Destek Üst Limiti: 300,000 TL / Destek Oranı: %60 https://www.kosgeb.gov.tr/site/tr/genel/detay/6797/destek-unsurlari		

7. Proje Yürütücüsü Bilgileri			
Unvanı, Adı Soyadı	Sedat ÖZTÜRK	GSM No	544 947 63 46
Bölümü	Bilgi Teknolojileri	Tarih	01/12/2024
Kurum sicil no	34-123456-78	İmza	
e-posta	sedat.ozturk3@ogr.sakarya.edu.tr		

8. Proje Ekibi

Unvanı, Adı Soyadı	Bölümü	Kurum sicil no	e-mail	İmza
Kadifeteks Mensucat A.Ş.	Yönetim / Sponsor	34-123456-01	info@kadifeteks.com	
Ömer ENDEN	Danışman	06-987654-32	omer@enderunakademi.gen.tr	
Sedat ÖZTÜRK	Proje Yöneticisi	34-123456-02	sedat.ozturk3@ogr.sakarya.edu.tr	
Ahmed Emin BALCI	Satın Alma	34-123456-03	ahmed.balci@ogr.sakarya.edu.tr	
Ahmet Can ŞAHİN	İnsan Kaynakları	34-123456-04	ahmet.sahin27@ogr.sakarya.edu.tr	
Enver YAMAN	Kalite Güvence	34-123456-05	enver.yaman@ogr.sakarya.edu.tr	
İsmail KARŞIĞA	Risk Yönetimi	34-123456-06	ismail.karsiga@ogr.sakarya.edu.tr	

9. PROJEYİ DESTEKLEYEN KURUMLAR / KURULUŞLAR			
Destekleyen kurum/kuruluş adı (1)	KOSGEB	Tarih	01/12/2024
Yetkilinin unvanı, adı soyadı	İstanbul İkitelli Müdürlüğü Karani İnce	İmza	
Telefon no	0212 454 07 01	Destek Miktarı (TL)	300,000 TL

10. ÖZET ve ANAHTAR KELİMELER:

ISO belgelendirme, uluslararası standartları karşılayan bir kalite yönetim sistemi veya başka bir yönetim sistemi standardına uyumu belgelendirme sürecidir. Bu belgeler, bir organizasyonun belirli standartlara uygun şekilde çalıştığını kanıtlar. "ISO" adı, International Organization for Standardization (Uluslararası Standardizasyon Örgütü) kelimelerinin kısaltmasıdır. ISO, 1947 yılında İsviçre'nin Cenevre kentinde kurulmuştur. Bu kuruluşun amacı, dünya çapında ticaretin ve iş birliğinin kolaylaştırılması için uluslararası standartlar geliştirmektir.

ISO belgeleri, Kalite, Güvenilirlik, Uluslararası Kabul, Müşteri Memnuniyeti, Yasal Uyumluluk, Verimlilik, Karlılık ve Rekabet Avantajı gibi sunduğu birçok özellik sebebiyle bir çok şirket tarafından tercih edilmektedir.

ISO standartlarının temel prensiplerinden biri olan "Yazdığını yap, yaptığını yaz" ifadesi, dokümantasyon ve uygulama sürecinin uyum içinde olmasını vurgular. Bu prensip, süreçlerin yazılı olarak tanımlanmasını, ardından bu tanımlamalara uygun şekilde uygulanmasını ve uygulamaların da kayıt altına alınmasını gerektirir. Böylece hem şeffaflık sağlanır hem de süreçlerin izlenebilirliği garanti altına alınır.

ISO 27001 standardı, bilgi güvenliği yönetim sistemleri (BGYS) için global olarak tanınan bir çerçeve sunmaktadır. Tarihsel olarak, bu standardın kökenleri 1990'larda yayımlanan BS 7799 (British Standards Institution, BSI) standardına dayanmaktadır. ISO tarafından 2005 yılında ISO/IEC 27001:2005 olarak kabul edilmiş ve 2013 ve 2022 yıllarında güncellenmiştir. Literatürde, bilgi güvenliğinin sistematik ve risk tabanlı yönetimini sağlayan temel bir referans noktası olarak konumlanmıştır. Bu standardın uygulanması, kurumsal süreçlerde bilgi güvenliği risklerini yönetmek ve paydaş güvenini artırmak açısından kritik öneme sahiptir. Araştırmanın özgün değeri, literatürdeki sektörel adaptasyon eksikliklerini gideren yeni metodolojiler sunmasında yatmaktadır. Bu bağlamda araştırma;

1. Fikri mülkiyet ve müşteri verilerinin korunmasına yönelik risk tabanlı yaklaşımlar sunulmasını,
2. Çalışan farkındalığını artırmaya yönelik sektör spesifik eğitim metodolojilerinin geliştirilmesini,
3. IoT ve dijitalleşen süreçlerdeki güvenlik açıklarını giderecek yeni kontrol mekanizmalarının tasarlanmasını hedefler.
4. Tedarik zinciri güvenliği için özelleştirilmiş bilgi güvenliği stratejileri geliştirilmesini,

ISO 27001 standardını kurumsal ihtiyaçlar doğrultusunda yenilikçi yaklaşımlarla uyarlamayı ve uygulanabilirlik analizlerini derinlemesine ele almayı hedeflemektedir. Literatürdeki eksiklerden biri, sektörel farklılıklara özgü ISO 27001 adaptasyonlarının yeterince ele alınmamış olmasıdır. Bu proje, sektörel farkları dikkate alarak bir metodoloji geliştirmeyi ve güvenlik süreçlerini optimize etmeyi amaçlamaktadır.

Beklenen Sonuçların Etkileri

1. **Kurumsal Güvenlik Kültürüne Katkı:** Bilgi güvenliği farkındalığını artırarak organizasyonların daha dirençli hale gelmesini sağlar.
2. **Rekabet Avantajı:** ISO 27001 belgesi, organizasyonlara uluslararası pazarlarda rekabet üstünlüğü sunar.
3. **Uyumluluk ve Yasal Risklerin Azaltılması:** Proje çıktıları, kuruluşların yasal ve düzenleyici gerekliliklere uyum sağlamalarını kolaylaştırır.
4. **Akademik Katkı:** Literatürde sektörel uyarlama ve uygulama örnekleri açısından bir boşluğu doldurur.

Projenin Yürütülme Süreci

1. **Yaklaşım:** Proje, ISO 27001 standardının sektörel adaptasyonunu değerlendirmek için hem nitel hem de nicel yöntemlerin kullanıldığı karma bir yaklaşım benimsemektedir. Nitel veriler uzman danışmanların görüşleri ve vaka analizlerinden, nicel veriler saha uygulamalarından elde edilecektir.
2. **Yöntemler**: ISO 27001'in sektörel uygulamaları incelenip eksiklikler belirlenecektir. Durum Analizi için Mevcut bilgi güvenliği yönetim süreçleri analiz edilmelidir. Özel risk değerlendirme ve kontrol yöntemleri geliştirilmelidir ve istatistiksel yöntemlerle sonuçlar değerlendirilecektir.
3. **Ekip :** ISO 27001 konusunda uzman bir akademisyen veya profesyonelin liderlik ettiği bir Proje Yöneticisi; bilgi güvenliği ve risk yönetimi alanlarında uzmanlaşmış bir Araştırma Ekibi; hedef sektörlerde deneyim sahibi Sektörel Danışmanlar ve veri toplama ile saha uygulamalarını gerçekleştiren Destek Personeli'nden oluşmaktadır.
4. **Aşamalar ve Zaman Çizelgesi:**
    a. **Proje Açılışı (1-2. Aylar):** Projenin tanıtımı ve hedeflerinin belirlenmesiyle başlanacaktır. Proje ekibi ve bilgi güvenliği ekibi atanarak koordinasyon sağlanacaktır.

b. **GAP Analizi (3-4. Aylar):** Mevcut durum analizi ve boşlukların tespit edilmesi için saha çalışmaları ve raporlama yapılacaktır. Bu aşamada organizasyonun mevcut bilgi güvenliği uygulamaları detaylı bir şekilde değerlendirilecektir..
c. **Eğitim (5-6. Aylar):** Bilgi güvenliği farkındalık eğitimi, ISO 27001 standart eğitimi ve iç denetçi eğitimi verilerek organizasyon genelinde bilgi güvenliği bilinci artırılacaktır.
d. **Risk Yönetimi (7-8. Aylar):** Bilgi varlıkları ve risk envanteri hazırlanacak, ardından bu varlıklara yönelik risk analizleri gerçekleştirilerek organizasyonun karşı karşıya olduğu potansiyel tehditler belirlenecektir.
e. **Dokümantasyon (9-10. Aylar):** ISO 27001'e uygun el kitabı, bilgi güvenliği politikaları, uygulanabilirlik bildirgesi (SoA), iş sürekliliği planı ve prosedürler hazırlanacaktır.
f. **Kontrol (11. Ay):** İç denetimler yapılacak, tespit edilen eksikliklere yönelik düzeltici faaliyetler uygulanacak ve yönetim gözden geçirme toplantıları düzenlenecektir.
g. **Belgelendirme (12. Ay):** Sertifikasyon için 1. ve 2. aşama denetimler gerçekleştirilecektir. Bu aşamaların başarılı tamamlanmasıyla ISO 27001 sertifikası alınması hedeflenmektedir.

Anahtar Kelimeler:

ISO/IEC 27001:2022, Bilgi Güvenliği Yönetim Sistemi (BGYS), Gap (Boşluk) Analizi, Risk Yönetimi, Dokümantasyon, Belgelendirme Süreci, İç Denetim, Sistem Tasarımı

11. AMAÇ:

Bu projenin temel amacı, ISO/IEC 27001:2022 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurarak organizasyonun bilgi varlıklarının korunmasını, bilgi güvenliği risklerinin sistematik ve etkin bir şekilde yönetilmesini sağlamaktır. Bununla birlikte, yasal ve düzenleyici gerekliliklere uyum sağlayarak firmanın bilgi güvenliği süreçlerini geliştirmek, kurumsal güvenlik kültürünü güçlendirmek ve uluslararası standartlara uygun bir yapı kazandırarak organizasyonun paydaş güvenini artırmak hedeflenmektedir. Proje kapsamında, firmanın uluslararası geçerliliğe sahip ve TÜRKAK akreditasyonlu bir belgelendirme kuruluşu tarafından denetlenmesi sonucunda ISO/IEC 27001:2022 BGYS belgesinin kazandırılması öngörülmektedir.

Süreç, firmanın bilgi güvenliği yönetiminde global düzeyde tanınan standartlara uygun bir seviyeye erişmesini sağlamanın yanı sıra, iş sürekliliğini destekleyen sistematik yaklaşımlar sunacaktır. Proje çıktıları arasında, IT süreçlerinin ve dokümantasyon altyapısının modernize edilmesi, organizasyonel yapıların optimize edilmesi ve çalışanlarda bilgi güvenliği bilincinin artırılması bulunmaktadır. Ayrıca, uluslararası pazarlarda firmanın güvenilirliğini ve rekabet avantajını artıracak bu sertifikasyon, organizasyonun uzun vadeli stratejik hedeflerine katkı sağlayacak önemli bir adım olarak değerlendirilmektedir.

12. KONU ve KAPSAM:

Bilgi, organizasyonlara değer katan ve bu nedenle korunması gereken kaynaktır. Bilişim sistemleri ve teknolojilerinin hızla gelişmekte ve değişmekte olduğu düşünüldüğünde bilişim sistemlerini organize ederken bilginin gizliliği, bütünlüğü ve erişilebilirliği firmamızda özel önem kazanmıştır. Firmamızın, her türlü bilginin elektronik ortamda tutulması ile birlikte bunun kullanımı, paylaşımı ve iletimi bilgi güvenliği açısından kritik öneme sahiptir. Bilginin kurumlar arasında iletişimi ve ayrıca internete açık olması bilgi güvenliği riskini daha fazla arttırmaktadır.

Bu sebeple ISO 27001:2022 standartlarına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurmayı, bu sistemi sürekli iyileştirmeyi ve firmanın bilgi güvenliği süreçlerini uluslararası standartlara taşıyarak belgelendirmeyi hedeflemektedir. Çalışma, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlamak amacıyla teknik ve yönetsel önlemleri kapsamaktadır.

Gizlilik	Önem taşıyan bilgilere yetkisiz erişimlerin önlenmesi

Bütünlük	Bilginin doğruluk ve bütünlüğünün sağlandığının gösterilmesi
Erişebilirlik	Yetkisi olanların gerektiği hallerde bilgiye ulaşılabilirliğinin gösterilmesi ilgili sistem standartları, sadece elektronik ortamda tutulan verilerin değil, yazılı, basılı, sözlü ve benzeri ortamda bulunan tüm verilerin güvenliği ile ilgilidir. Standart, firma ölçeği, sektör, iş süreçlerinin farklılığı gibi konulara bakılmaksızın bütün kuruluşlar için uygulanabilir özelliktedir.

Bilgi Güvenliği Yönetim Sistemi, firmanın şahsına, müşterilerine ve tedarikçilerine ait tüm bilgi varlıklarının güvenliğini kapsar. Firmamızın bütün çalışanları, sözleşmeleri ve firmamız adı altında çalışan bütün kişi, alt yüklenici firmaları ve operasyonda kullanılan tüm elektronik ortamlar için geçerlidir. Aynı zamanda işletmemizin sahip olduğu ve kiraladığı bütün cihazlar içinde geçerlidir.

Proje, üç temel aşamadan oluşmaktadır:

1. **Dokümantasyon:** ISO 27001 BGYS standardı gerekliliklerine uygun şekilde bilgi güvenliği yönetim sisteminin tasarlanması, süreçlerin analiz edilmesi ve gerekli politikalar, prosedürler, talimatlar ile diğer dokümanların hazırlanması gerçekleştirilmiştir.
2. **Eğitim:**
    a. **Bilgi Güvenliği Farkındalık Eğitimleri:** Çalışanların bilgi güvenliği bilincini artırmak ve günlük operasyonlarda güvenlik odaklı bir yaklaşımı benimsemelerini sağlamak amacıyla farkındalık eğitimleri düzenlenmiştir.
    b. **Uzman Eğitimleri:** Bilgi İşlem Ekibine, ISO 27001 BGYS standartları ve iç denetim süreçlerine yönelik teknik ve uygulamalı eğitimler verilmiştir.
3. **Belgelendirme:** Oluşturulan Bilgi Güvenliği Yönetim Sistemi (BGYS), uluslararası akreditasyona sahip bir belgelendirme kuruluşu (TÜRKAK akreditasyonlu) tarafından denetlenmiş ve standartlara uygunluğu doğrulanarak ISO 27001 BGYS belgesi alınmıştır.

13. LİTERATÜR ÖZETİ:

ISO 27001 standardının literatürdeki önemi, bilgi güvenliğini yönetmenin sadece teknik değil aynı zamanda yönetsel bir süreç olduğunu vurgulamaktadır. Yani; bilgi güvenliği yönetiminin yalnızca teknolojik önlemlerle (antivirüs, güvenlik duvarları, şifreleme vb.) sınırlı değil, aynı zamanda stratejik planlama, organizasyonel yapılar ve politikalar gibi yönetsel unsurları da ilgilendirmektedir.

Literatürdeki Çalışmaları

1. **Organizasyonel Kazanımlar:** ISMS (Information Security Management System) kurulumunun, organizasyonların bilgi güvenliğine yönelik tehditlere karşı dayanıklılığını artırdığı vurgulanmıştır. Özellikle dijitalleşmenin arttığı ve siber saldırıların yaygınlaştığı bir dönemde, standartın uygulanmasının organizasyonel risk yönetiminde önemli rol oynadığı belirtilmektedir.
   Kaynak: *Peltier, T. R. (2016). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management.*

   Peltier, bilgi güvenliği kuruluşunuzun değerli bilgi kaynaklarını korumak için olduğu söyler. Ancak çoğu zaman bilgi güvenliği çabaları iş hedeflerini engellemek olarak görülür. Etkili bir bilgi güvenliği programı bilgi varlıklarınızı korur ve iş hedeflerinize ulaşmanıza yardımcı olur. Bilgi Güvenliği Politikaları, Prosedürleri ve Standartları, Etkili Bilgi Güvenliği Yönetimi İçin Kılavuzlar, bir sıkıntı olarak değil, kuruluşunuzun hedeflerine ulaşmanın bir yolu olarak görülecek bir güvenlik programını seçmeniz, geliştirmeniz ve uygulamanız için ihtiyaç duyduğunuz araçları sağlar.

2. **Uyum ve Yasal Gereklilikler:** Literatürde ISO 27001'in GDPR gibi veri koruma düzenlemeleriyle uyumda kritik bir araç olduğu vurgulanmaktadır. Humphreys (2021), bu standardın kişisel verilerin korunmasına yönelik yasal gereklilikleri karşılamada organizasyonlara rehberlik ettiğini belirtmiştir.
   Kaynak: *Humphreys, 2021*

Edward Humphreys, bilgi güvenliği yönetim sistemleri (ISMS) ve ISO/IEC 27001 standardının geliştirilmesinde öncü bir uzmandır. Uluslararası Telekomünikasyon Birliği'ne (ITU) göre, Humphreys, ISMS standartlarının uluslararasılaştırılması ve ISMS sertifikasyonunun geliştirilmesi konusundaki çalışmalarıyla tanınmaktadır.

Literatürdeki Boşluklar ve Araştırma İhtiyaçları

ISO 27001 standardına ilişkin literatürde dikkat çeken boşluklar ve bu projenin önemini destekleyen unsurlar şunlardır:

1. **Kurumlara Özel Uyarlamalar:** Literatür, ISO 27001'in farklı organizasyonel yapılar ve sektörlerde uygulanmasına dair genel yaklaşımlar sunarken, kuruma özel uyarlamalar konusunda sınırlı bilgi sağlamaktadır. Bu durum, proje kapsamında kuruma özgü bir BGYS tasarımının gerekliliğini desteklemektedir.

   Kaynak: *AlHogail (2018). ""Improving information security awareness: Student perceptions of information security"" isimli makalesinde bu konuya dikkat çekerek, kuruma özel risk değerlendirme ve kontrol mekanizmalarının geliştirilmesinin zorunluluğunu vurgulamaktadır.*

   Organizasyonların farklı yapısal ihtiyaçlarına göre BGYS'nin özelleştirilmesi ve uygulamada karşılaşılan zorlukların analiz edilmesi gerekmektedir. Bu proje, kuruma özel bir BGYS modeli geliştirerek, bu boşluğun doldurulmasına katkı sağlamayı amaçlamaktadır.

2. **Süreçlerin Sürdürülebilirliği:** ISO 27001 sistemlerinin uygulanmasından sonraki sürdürülebilirlik aşamalarına yönelik çalışmaların eksik olduğu görülmektedir

   Kaynak: *Siponen & Willison (2009), "Information Security Management Standards: Problems and Solutions" isimli makalesinde BGYS'nin sürdürülebilir yönetimi için gerekli olan süreçlerin göz ardı edildiğini belirtmektedir.*

   BGYS uygulamalarının uzun vadeli sürdürülebilirliğini sağlayacak mekanizmaların (örneğin sürekli eğitim, performans değerlendirme, iç denetim süreçleri) geliştirilmesi ve bu mekanizmaların etkinliğinin ölçülmesi gereklidir. Proje kapsamında sürdürülebilir BGYS modellerinin tasarımı bu boşluğu dolduracaktır.

3. **Çalışan Farkındalığı:** Çalışanların bilgi güvenliği farkındalığına dair eğitimlerin etkinliği ve etkileri üzerine yapılan çalışmalar sınırlıdır (Kritzinger & Smith, 2008). Bu proje, bu alanlardaki eksikliklere de yanıt sunmayı hedeflemektedir.

   Kaynak: *Kritzinger & Smith (2008)." Information security management: An information security retrieval and awareness model for industry" isimli makalesinde bu konuda yapılan çalışmaların yetersizliğine dikkat çekmektedir.*

   Çalışan farkındalığını artırmak için daha etkili eğitim yöntemlerinin geliştirilmesi, çalışan davranışlarının nasıl değiştiğinin ölçülmesi ve organizasyonun genel bilgi güvenliği kültürüne etkilerinin analiz edilmesi gerekmektedir. Proje, bu eksikliğe odaklanarak, çalışanların farkındalık düzeyini artırmak için somut çözüm önerileri geliştirmeyi hedeflemektedir.

14. ÖZGÜN DEĞER:

Bu araştırma, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardının kuruma özgü uyarlanması ve sürdürülebilir bir bilgi güvenliği altyapısının oluşturulması konusuna odaklanmaktadır. Araştırmanın temel hipotezi, "ISO 27001:2022'nin kurumsal yapı ve ihtiyaçlara uygun bir şekilde uygulanmasının, bilgi güvenliği risklerini etkili bir şekilde yöneterek organizasyonel dayanıklılığı artıracağı"dır. Ayrıca, sistemin sürdürülebilirliği ve çalışan farkındalığı gibi unsurların iyileştirilmesiyle bilgi güvenliği yönetiminde daha kalıcı ve etkin sonuçlar elde edileceği öngörülmektedir.

Araştırmanın özgün değeri, mevcut literatürdeki boşlukları dolduracak yeni yaklaşımlar ve metodolojiler sunmasından kaynaklanmaktadır:

1. **Kuruma Özel Uyarlama:** Literatürde ISO 27001'in genel uygulamalarına dair geniş bilgi bulunmakla birlikte, standartın organizasyonel yapı ve sektörel farklılıklara göre nasıl özelleştirilebileceği konusunda sınırlı bilgi yer almaktadır. Bu çalışma, firmanın operasyonel süreçlerine uygun, özelleştirilmiş bir BGYS modelinin nasıl tasarlanabileceğini detaylandırarak literatüre katkı sağlamaktadır.

2. **Sürdürülebilirlik ve Etkililik:** Araştırma, sadece bir BGYS kurulumu değil, aynı zamanda bu sistemin uzun vadeli sürdürülebilirliği için metodolojik bir çerçeve sunmaktadır. Bu çerçeve, ISO 27001 sistemlerinin uygulama sonrası süreçlerdeki etkinliğini artırmaya yönelik yeni bir yaklaşım ortaya koymaktadır.

3. **Çalışan Farkındalığı ve Eğitim:** Literatürde, bilgi güvenliği farkındalığı eğitimlerinin etkinliği sınırlı düzeyde ele alınmıştır. Bu araştırma, hem çalışan farkındalığını artırmaya yönelik yenilikçi eğitim modelleri hem de eğitimlerin etkisini ölçmek için kullanılabilecek metrikler geliştirilmesini önermektedir.

4. **Risk Yönetimi ve Teknolojik Uygulamalar:** ISO 27001:2022'nin sunduğu esnek risk yönetimi yaklaşımı, proje kapsamında uygulamalı olarak incelenecek ve bu bağlamda yeni bir metodoloji geliştirilecektir. Özellikle KOBİ'ler ve farklı sektörlere uygulanabilir, daha basitleştirilmiş bir model önerilmektedir.

Araştırmanın literatüre katkısı, hem standartların daha geniş bir kurumsal yelpazede uygulanabilirliğine dair somut örnekler sunması hem de bilgi güvenliği yönetim sistemleri alanında daha özelleştirilmiş, sürdürülebilir ve eğitim odaklı çözümler üretmesidir. Böylece, bilgi güvenliği süreçlerinin etkinliğini artırarak organizasyonel başarıya ve uluslararası standartlara uyuma yeni bir perspektif kazandırılması hedeflenmektedir.

15. YÖNTEM:

Bu araştırma, ISO 27001:2022 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) kuruma özgü tasarlanması, uygulanması ve belgelendirilmesi için yapılandırılmıştır. Çalışma, hem teorik hem de uygulamalı bir yaklaşımla yürütülecek olup, araştırmanın tasarımı ve incelenmek üzere seçilen parametreler aşağıda detaylandırılmıştır.

1. **Araştırmanın Tasarımı ve Yaklaşımlar**
   Araştırma üç temel aşamadan oluşmaktadır: Dokümantasyon, Eğitim ve Belgelendirme. Her aşama için incelenecek parametreler, yöntemler ve kullanılacak materyaller şu şekilde yapılandırılmıştır:

2. **İncelenecek Parametreler**
   Araştırmanın kapsamı ve amaçları doğrultusunda şu parametreler seçilmiştir:

   a. **Bilgi Güvenliği Riskleri:** Organizasyonun iş süreçlerinde karşı karşıya olduğu riskler (teknik, yönetsel, çevresel).
   b. **Mevcut Durum Analizi:** Bilgi güvenliği altyapısındaki eksiklikler, politika ve prosedürlerdeki boşluklar.
   c. **Dokümantasyon İhtiyaçları:** ISO 27001 gerekliliklerine uygun prosedürler, talimatlar ve politikaların belirlenmesi.
   d. **Çalışan Farkındalığı ve Eğitim Seviyesi:** Çalışanların bilgi güvenliği bilinci ve standartlarla uyumu.
   e. **BGYS Performansı:** Uygulanan sistemin etkinliği, sürdürülebilirliği ve uyumluluk düzeyi.
   f. **Uygulama Alanları ve Entegrasyon:** Farklı departmanların (Bilgi İşlem, İthalat-İhracat, Muhasebe vb.) BGYS entegrasyonu.

3. Uygulanacak Yöntem ve Kullanılacak Materyal

Yöntem	Metot	Materyal
Mevcut Durum Analizi	• Organizasyonel bilgi varlıklarının detaylı bir envanteri çıkarılacak. • Risk değerlendirme ve etki analizi (RA/RIA) yapılacak. • Çalışmalar ISO 27001'in Annex A kontrol setleriyle karşılaştırılarak eksikler belirlenecek.	• Risk değerlendirme ve analiz yazılımları. • Organizasyonun bilgi işlem altyapısı, mevcut politikalar ve prosedürler.
Dokümantasyon Süreci	• ISO 27001:2022 gerekliliklerine göre bilgi güvenliği politikaları, prosedürleri, talimatları ve formlar hazırlanacak. • Her doküman, iş süreçlerine entegre edilecek şekilde tasarlanacak.	• Standart şablonlar ve ISO 27001 uyum araçları. • Firma süreçlerine dair organizasyon şemaları ve iş akışları.
Farkındalık ve Uzman Eğitimleri	• Tüm çalışanlara bilgi güvenliği bilincini artıracak interaktif ve uygulamalı eğitimler düzenlenecek. • ISO 27001'in iç denetim süreçleri ve teknik detayları hakkında bilgi işlem ekibine uygulamalı eğitimler verilecek.	• Görsel-işitsel içerikler, simülasyonlar ve eğitim modülleri. • Teknik rehberler ve uygulama yazılımları.
Risk Yönetimi	• Varlık envanterinin hazırlanması. • Risk envanterinin oluşturulması. • Risk analizi ve değerlendirmesi yapılması.	• Risk yönetimi yazılımları. • Varlık ve risk envanter formları.
Kontrol	• İç denetimlerin gerçekleştirilmesi. • Düzeltici faaliyetlerin planlanması ve uygulanması. • Yönetimin gözden geçirme toplantılarının yapılması.	• Denetim raporları ve kontrol listeleri. • Düzeltici faaliyet formları. • Toplantı tutanakları.
Belgelendirme Süreci	• ISO 27001:2022 gereklilikleri doğrultusunda oluşturulan BGYS'nin bir ön denetimden geçirilmesi. • Uluslararası akreditasyona sahip belgelendirme kuruluşu tarafından nihai denetim yapılacak.	• TÜRKAK akreditasyonlu bir belgelendirme kuruluşunun sağladığı denetim materyalleri. • BGYS dokümantasyonu ve risk yönetimi raporları.

4. Verilerin Toplanması ve Ölçümler

a. Risk Değerlendirme ve Yönetimi:
Bilgi varlıklarına yönelik tehdit türleri, bu tehditlerin etki ve olasılık düzeyleri belirlenmelidir. Sonrasında "Etki x Olasılık" matrisi kullanılarak risk önceliklendirme yapılmalıdır.

b. Çalışan Farkındalığı Seviyesi:
Eğitim öncesi ve sonrası yapılan anketlerle bilgi güvenliği farkındalığı düzeyi ölçülecektir. Sonrasında Eğitim etkinliği yüzdesel başarı ile değerlendirilecektir.

c. BGYS Performansı:
Uygulama sonrası ihlal oranları, sistemin iş süreçlerine entegrasyon düzeyi belirlenecektir. Sonrasında Yıllık bilgi güvenliği olay raporları analiz edilerek ölçülecektir.

5. **Kurulacak İlişkiler**
   Risk değerlendirme sonuçları ile önerilen kontrol mekanizmaları arasındaki ilişki analiz edilecektir. Çalışan farkındalığı düzeyindeki artışın, bilgi güvenliği ihlal oranlarına etkisi ölçülecektir. Dokümantasyon sürecinde oluşturulan politika ve prosedürlerin, denetim sürecindeki uygunluğu değerlendirilecektir.

Bu yöntemle, ISO 27001:2022'ye uyumlu bir BGYS'nin kuruma özgü ihtiyaçlarla nasıl entegre edileceği sistematik bir şekilde ortaya konulacaktır.

16. ARAŞTIRMA OLANAKLARI:

Bu projede, ISO 27001:2022 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi'nin (BGYS) kurulumu ve belgelendirilmesi için gerekli altyapı, ekipman ve insan kaynağı olanakları etkin bir şekilde kullanılacaktır. Projeyi destekleyecek araştırma olanakları şu şekilde sıralanmıştır:

1. **Altyapı Olanakları**
   a. **Bilgi İşlem Altyapısı:** Organizasyonun mevcut ağ yapısı, sunucuları, veri depolama sistemleri ve bilgi işlem altyapısı projede risk değerlendirme ve yönetim süreçleri için kullanılacaktır. Sistemlerin mevcut güvenlik açıklarını değerlendirmek için kullanılan güvenlik duvarları, antivirüs yazılımları ve log yönetim sistemleri gibi araçlar projeye entegre edilecektir.
   b. **Veri Analizi ve Yönetimi:** BGYS'ye ilişkin süreçlerin dokümantasyonu, analiz edilmesi ve optimize edilmesi için kullanılan mevcut ERP sistemleri, iş akış araçları ve raporlama yazılımları proje sürecinde etkin bir şekilde değerlendirilecektir.
   c. **Denetim ve Uygunluk Araçları:** Projede kullanılacak denetim araçları, BGYS'nin ISO 27001:2022 gerekliliklerine uygunluğunu ölçmek için kullanılacak uluslararası standartlara uygun uyum kontrol listelerini içerir.
2. **Ekipman Olanakları**
   a. **Teknolojik Ekipmanlar:** Çalışmalar sırasında mevcut donanımlar (dizüstü bilgisayarlar, sunucular, mobil cihazlar) analiz, test ve eğitim süreçleri için kullanılacaktır. Siber güvenlik risk değerlendirme yazılımları ve simülasyon araçları, kontrol mekanizmalarının uygulanabilirliğini değerlendirmek için kullanılacaktır.
   b. **Eğitim Materyalleri:** Çalışanlar için düzenlenecek farkındalık ve uzman eğitimlerinde kullanılacak görsel-işitsel eğitim araçları, e-öğrenme platformları ve interaktif simülasyon materyalleri mevcuttur.
3. **İnsan Kaynağı ve Uzmanlık**
   a. **Bilgi Güvenliği Ekibi:** Kurum bünyesindeki bilgi işlem birimi, mevcut güvenlik altyapısının değerlendirilmesi ve BGYS'nin teknik uygulamalarının gerçekleştirilmesi için kullanılacaktır. İç denetim ekibi, standardın denetim gerekliliklerini karşılamak üzere eğitilecek ve sürece dahil edilecektir.
   b. **Danışmanlık ve Harici Destek:** Uluslararası akreditasyona sahip belgelendirme kuruluşları (TÜRKAK onaylı) ile iş birliği yapılacaktır. Bu kuruluşların denetim ekipmanları ve metodolojilerinden faydalanılacaktır.
4. **Eğitim ve Dokümantasyon Olanakları**
   a. **Eğitim Olanakları:** Çalışanlar için kurum içinde düzenlenecek farkındalık eğitimleri için hazırlanmış interaktif ve çevrimiçi eğitim modülleri mevcuttur. Teknik ekip için detaylı BGYS iç denetim eğitimleri, ulusal ve uluslararası bilgi güvenliği eğitmenlerinden alınacaktır.
   b. **Dokümantasyon Altyapısı:** Organizasyonun mevcut belge yönetim sistemi, standart gerekliliklerine uygun prosedür, politika ve talimatların hazırlanması ve saklanması için kullanılacaktır.

5. **İşbirlikçi Olanaklar**
    a. **Akreditasyonlu Kurumlarla İşbirliği:** ISO 27001 belgelendirme sürecinde TÜRKAK akreditasyonlu bir belgelendirme kuruluşu, sistemin uygunluğunu değerlendirmek için süreçlere dahil edilecektir.
    b. **Endüstri Uzmanları:** Kritik süreçlerin oluşturulmasında bilgi güvenliği uzmanları, risk analistleri ve süreç yöneticilerinin deneyimlerinden faydalanılacaktır.

Bu araştırma olanakları, BGYS'nin kuruma özgü şekilde başarılı bir şekilde tasarlanmasını ve uygulanmasını desteklemek için gerekli tüm altyapı ve uzmanlık ihtiyaçlarını karşılamaktadır. Proje boyunca mevcut olanaklar optimize bir şekilde kullanılacak, gerektiğinde ilave uzmanlık ve araçlardan faydalanılacaktır.

Projede Kullanılacak Mevcut Makine – Teçhizat Listesi (*)	
Adı/Modeli	**Projede Kullanım Amacı**
Dell PowerEdge R740	Bilgi güvenliği yönetim sistemi için sunucu altyapısının sağlanması, veri işleme ve saklama işlemleri.
Lenovo ThinkPad P15 Gen 2	Risk analizi, dokümantasyon ve eğitim materyallerinin hazırlanması
Microsoft Surface Hub 2S	Çalışan farkındalık eğitimlerinde interaktif sunumların yapılması.
FortiGate 100F	Siber güvenlik önlemlerinin uygulanması, veri erişim kontrollerinin yapılandırılması.
HP LaserJet Pro MFP M428	Dokümantasyon süreçlerinde prosedür, politika ve talimatların yazdırılması ve çoğaltılması.
Brother ADS-2700W Tarayıcı	Fiziksel dokümanların dijitalleştirilmesi ve BGYS dokümantasyonuna entegre edilmesi.
APC Smart-UPS C 1500VA	Sunucu ve ağ cihazlarının kesintisiz güç kaynağıyla çalıştırılması, veri kaybının önlenmesi.

17. YAYGIN ETKİ/KATMA DEĞER:

Projenin sağladığı katma değer ve beklenen yaygın etkiler şu şekilde sıralanabilir:

1. **Ulusal Ekonomiye Katkı**
    a. **Rekabet Gücünün Artırılması:** ISO 27001:2022 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) oluşturulması, kurumun uluslararası ticarette güvenilir bir iş ortağı olarak konumlanmasına olanak sağlayacaktır. Bu durum, özellikle bilgi güvenliğinin kritik olduğu sektörlerde (örneğin finans, sağlık, enerji) kurumsal itibarın artmasına ve ekonomik büyümeye katkıda bulunacaktır.
    b. **Siber Risklerin Azaltılması:** Proje, bilgi güvenliği açıklarının minimize edilmesiyle siber saldırıların neden olduğu ekonomik kayıpları önlemeye yardımcı olacaktır.
    c. **Küçük ve Orta Ölçekli İşletmelere (KOBİ) Model:** Proje sonucunda oluşturulacak BGYS yapısı, KOBİ'ler için esnek ve uygulanabilir bir bilgi güvenliği yönetim modeli sunarak, onların bilgi güvenliği standartlarına ulaşmasına destek olacaktır.

2. **Toplumsal Refah**
    a. **Veri Güvenliği ve Kişisel Verilerin Korunması:** ISO 27001'in uygulanmasıyla bireylerin kişisel verilerinin güvenliğinin artırılması, toplumsal güven duygusunu güçlendirecektir.
    b. **İstihdam Olanakları:** Proje kapsamında edinilecek bilgi güvenliği uzmanlığı, yetişmiş insan kaynağı ihtiyacını karşılayarak yeni istihdam fırsatları yaratacaktır.

c. **Bilgi Güvenliği Farkındalığı:** Proje sürecinde düzenlenen eğitimler ve farkındalık çalışmaları, toplumsal düzeyde bilgi güvenliği bilincini artıracak ve bireylerin dijital ortamda daha güvenli hareket etmelerini sağlayacaktır.

3. Bilimsel Birikime Katkı

a. **Uygulamalı BGYS Modeli: Proje,** ISO 27001 standardının kuruma özgü uyarlanması için geliştirilen yenilikçi metodolojilerle bilimsel literatüre katkı sağlayacaktır.
b. **Yenilikçi Eğitim Yaklaşımları :** Çalışan farkındalığını artırmak için geliştirilen eğitim ve değerlendirme yöntemleri, bilgi güvenliği farkındalığı alanında yeni uygulamalara kapı açacaktır.
c. **Sürdürülebilirlik Perspektifi :** Bilgi güvenliği sistemlerinin sürdürülebilir şekilde uygulanmasına yönelik öneriler, akademik çalışmalar ve uygulamalı projeler için yol gösterici olacaktır.

4. Elde Edilecek Sonuçlardan Yararlanacak Kesimler

a. **Kurumlar:** Belgelendirme sonucunda organizasyonlar, uluslararası bilgi güvenliği standartlarına uygun çalışarak itibar ve güvenilirlik kazanacaktır.
b. **Çalışanlar:** Çalışanların bilgi güvenliği farkındalıklarının artması, iş süreçlerinde daha dikkatli ve güvenli bir yaklaşım benimsemelerine katkı sağlayacaktır.
c. **Toplum:** Verilerin güvenliğiyle bireylerin gizlilik hakları korunacak ve dijitalleşen toplumsal süreçlerde daha güvenli bir ortam sağlanacaktır.
d. **Akademi ve Uygulayıcılar:** Araştırma çıktıları, akademisyenlere ve bilgi güvenliği uzmanlarına rehberlik ederek sektörel uygulamaları geliştirecektir.

Bu model, bilgi güvenliği ihlallerini azaltarak kurumsal süreçlerin verimliliğini artıracak, ulusal ekonomiye katkıda bulunacak ve bireyler ile toplumda güvenli bir dijital ortamın oluşumuna öncülük edecektir.

18. ÇALIŞMA TAKVİMİ:

İŞ-ZAMAN ÇİZELGESİ (1. YIL)													
İş Paketi Ad/Tanım			AYLAR										
			1	2	3	4	5	6	7	8	9	10	11	12
1	**Proje Açılış**													
	1.1	Proje Tanıtımı	■											
	1.2	Proje Ekibinin Belirlenmesi	■											
	1.3	BG Ekibinin Ataması	■											
2	**GAP Analizi**													
	2.1	Mevcut Durum Tespiti	■											
	2.2	Boşluk Analizi	■											
	2.3	Raporlama	■											
3	**Eğitim**													
	3.1	Farkındalık Eğitimi		■										
	3.2	ISO 27001 Standart Eğitimi					■							
	3.3	ISO 27001 İç Denetçi Eğitimi									■			
4	**Risk Yönetimi**													
	4.1	Varlık Envanterinin Hazırlanması		■										
	4.2	Risk Envanterinin Hazırlanması			■									
	4.3	Risk Analizi			■									
5	**Dokümantasyon**													

	5.1	ISO 27001 El Kitabı				■								
	5.2	ISO 27001 BG Politikaları				■								
	5.3	Uygulanabilirlik Bildirgesi (SoA)					■							
	5.4	İş Sürekliliği Planı					■							
	5.5	ISO 27001 BG Prosedürleri						■	■	■	■			
6	**Kontrol**													
	6.1	İç Denetim										■		
	6.2	Düzeltici Faaliyetler										■		
	6.3	Yönetimi Gözden Geçirme											■	
7	**Belgelendirme**													
	7.1	1. Aşama Denetim												■
	7.2	2. Aşama Denetimi												■

19. BAŞARI ÖLÇÜTLERİ:

Projenin tam anlamıyla başarıya ulaşması, ISO 27001:2022 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardına uygun bir sistemin kurulması, uygulanması ve belgelendirilmesi için belirlenen iş paketlerinin eksiksiz ve zamanında tamamlanmasına bağlıdır. Bu kapsamda, her bir iş paketi için belirlenen başarı ölçütleri, önem dereceleri ve projeye olan katkıları şu şekilde açıklanmıştır:

Ölçüt	Başarı Ölçütleri	Önem Derecesi	Proje Katkısı
Mevcut Durum Analizi ve Risk Değerlendirmesi	• Bilgi varlıklarının eksiksiz bir envanterinin çıkarılması • Organizasyonun bilgi güvenliği risklerinin tespit edilmesi ve her risk için olasılık ve etki değerlendirmesi yapılması. • Risk yönetim planının hazırlanması.	Çok Yüksek	Bu iş paketi, projenin temel altyapısını oluşturur. Mevcut durumun doğru bir şekilde analiz edilmesi, sonraki tüm adımların doğruluğunu ve etkinliğini doğrudan etkiler
Dokümantasyon Süreci	• ISO 27001:2022 standardına uygun politika, prosedür, talimat ve formların hazırlanması. • Dokümantasyonun kurumsal süreçlere entegre edilmesi ve ilgili birimlere dağıtılması.	Yüksek	Organizasyonel süreçlerin standartlara uygun bir şekilde yürütülmesi sağlanır ve belgelendirme denetiminde uyumluluk doğrulanır.
Eğitim Faaliyetleri	• Tüm çalışanlara bilgi güvenliği farkındalık eğitimlerinin verilmesi. • Teknik ekibe, ISO 27001 standardı ve iç denetim süreçlerine yönelik uygulamalı eğitimlerin tamamlanması. • Eğitimlerin etkinliğinin ölçülmesi (ör. öncesi ve sonrası farkındalık testleri).	Orta-Yüksek	Çalışanların bilgi güvenliği bilincinin artmasıyla sistemin güvenliği ve sürdürülebilirliği desteklenir.
Uygulama ve Entegrasyon	• BGYS'nin organizasyonel süreçlere tam entegrasyonunun sağlanması. • Risk yönetimi planında belirlenen kontrol mekanizmalarının uygulanması. • Sistemlerin test edilmesi ve aksaklıkların giderilmesi.	Çok Yüksek	Organizasyonun bilgi güvenliği risklerine karşı dayanıklılığı artırılır ve sistem işleyişine güven sağlanır.
İç Denetim ve Ön	• İç denetimlerin planlanması ve gerçekleştirilmesi.	Yüksek	Denetim öncesi olası eksikliklerin giderilmesiyle belgelendirme

Değerlendirme	• Tespit edilen uygunsuzlukların giderilmesi için düzeltici ve önleyici faaliyetlerin tamamlanması. • Belgelendirme denetimine hazır hale gelinmesi.		sürecinin başarı oranı artırılır.
Belgelendirme Süreci	• TÜRKAK akreditasyonlu bir belgelendirme kuruluşu tarafından gerçekleştirilen denetimin başarılı tamamlanması. • ISO 27001:2022 belgesinin alınması.	Çok Yüksek	Organizasyonun ulusal ve uluslararası pazarda bilgi güvenliği açısından güvenilir bir kurum olarak tanınmasını sağlar.
İzleme ve Sürekli İyileştirme	• Belgelendirme sonrası düzenli olarak iç denetimlerin yapılması. • İyileştirme fırsatlarının tespit edilmesi ve uygulanması	Orta	Bilgi güvenliği yönetiminin sürekliliği sağlanır ve sistemin etkinliği artırılır.

Bu ölçütler, projenin somut çıktılarının ölçülmesine ve başarıya ulaşmasına sağlar.

B PLANI:

Projede belirlenen iş paketlerinde beklenmeyen aksaklıklar veya başarısızlık durumlarında devreye alınabilecek alternatif stratejiler aşağıda iş paketlerine göre sıralanmıştır.

Ölçüt	Beklenebilecek Sorunlar	B Planı
Mevcut Durum Analizi ve Risk Değerlendirmesi	Bilgi varlıklarının envanterinin eksik veya yanlış çıkarılması, risk değerlendirme süreçlerinde yeterli veri toplanamaması.	• Eksik bilgi varlıklarının tespiti için departman yöneticileriyle ek görüşmeler yapılacak. • Harici danışmanlık firmalarından destek alınarak risk değerlendirme süreçleri hızlandırılacak. • Daha basit bir risk yönetimi modeli (ör. temsili varlık analizi) uygulanarak kısa vadeli çözümler üretilecek.
Dokümantasyon Süreci	Dokümantasyonun kapsamlı ve standartlarla uyumlu olmaması, sürecin zamanında tamamlanamaması.	• Belgelendirme kuruluşu veya dış kaynaklı uzmanlardan ISO 27001 uyumlu şablon ve rehber doküman desteği alınacak. • Kritik dokümanlara (politikalar, risk yönetimi prosedürleri vb.) öncelik verilerek dokümantasyon kademeli tamamlanacak. • Prosedürlerin sadeleştirilmesi ve temelde gerekli olan asgari belgelerin hazırlanması sağlanacak.
Eğitim Faaliyetleri	Eğitimlerin çalışanlara ulaşamaması, katılım oranlarının düşük olması veya eğitimlerin etkisiz olması.	• Çevrimiçi eğitim platformları (ör. video konferans araçları veya e-öğrenme sistemleri) devreye alınacak. • Eğitim içeriği sadeleştirilerek çalışanların daha hızlı adapte olabileceği bir format oluşturulacak. • Eğitim öncesi ve sonrası anketlerle odaklanılması gereken konular tespit edilip, revize edilmiş eğitimler sunulacak.
Uygulama ve Entegrasyon	BGYS'nin iş süreçlerine entegrasyonunda teknik veya yönetsel zorlukların yaşanması.	• Daha basit ve düşük maliyetli kontrol mekanizmaları (ör. manuel kontroller veya öncelikli risklere odaklanma) geçici olarak devreye alınacak. • Entegrasyon önceliği yüksek olan birimlere odaklanılarak, aşamalı uygulama modeli kullanılacak. • Harici BT uzmanlarından veya standart entegrasyon yazılımlarından destek alınacak.
İç Denetim ve Ön Değerlendirme	İç denetimlerde çok sayıda uygunsuzluk tespit edilmesi veya düzeltici faaliyetlerin zamanında	• İç denetim bulguları önem derecesine göre sıralanarak, yüksek öncelikli sorunlara odaklanılacak. • Düzeltici faaliyetlerin bir kısmı denetim öncesinde planlanarak, denetim sırasında eksikliklerin giderilmesi için süre kazanılacak.

	tamamlanamaması.	• Denetim sonuçlarının bir kısmı için dış danışmanlık firmalarından destek alınacak.
Belgelendirme Süreci	Belgelendirme denetiminde eksikliklerin tespit edilmesi ve belgelendirme sürecinin gecikmesi.	• Belgelendirme denetimi öncesinde tekrar bir ön denetim planlanarak eksikliklerin belirlenmesi sağlanacak. • Eksikliklerin kısa sürede giderilebilmesi için belgelendirme kuruluşundan rehberlik talep edilecek. • Denetim sonrası uygunsuzluk giderme sürecinde, acil ve önemli kontroller önceliklendirilerek denetim tekrarı yapılacak.
İzleme ve Sürekli İyileştirme	Sistem izleme ve iyileştirme süreçlerinin aksaması veya planlanandan daha yavaş ilerlemesi.	• Periyodik izleme süreçleri daha az sıklıkta yapılacak şekilde revize edilerek iş yükü hafifletilecek. • Öncelikli risklere odaklanılarak izleme kapsamı daraltılacak. • İç denetim ekibi veya bilgi işlem birimine sistem takibi için ek yazılım araçları sağlanacak.

Projede olası aksaklıkların etkisini minimize etmeyi ve hedeflere ulaşmayı sağlamak amacıyla alternatif stratejiler sunmaktadır.

20. Projedeki Görevlerin Dağılımı ve Birimin Özellikleri

Öneri Sahipleri Adı Soyadı	Katkı Oranı (%)	Görev alacağı aşamalar	Konuyla İlgili Araştırma Deneyimi ve Görev Aldığı Diğer Projeler (Varsa)
Danışman Ömer ENDEN	%15	• ISO 27001 standardı kapsamında süreçlerin uyumluluğunu denetleme. • Risk değerlendirme süreçlerinde uzman görüşü sağlama. • Eğitim materyallerinin hazırlanmasında teknik destek sunma.	• ISO 27001 belgelendirme süreçlerinde danışmanlık deneyimi bulunmaktadır. • Bilgi güvenliği ve yönetim sistemleri konusunda akademik çalışmaları bulunmaktadır.
Proje Yöneticisi Sedat ÖZTÜRK	% 25	• Projenin genel koordinasyonu ve yönetimi. • ISO 27001 BGYS gerekliliklerine uygun süreçlerin planlanması ve uygulanması. • İç ve dış iletişimin sağlanması, ekiplerin ilerleme durumlarının takibi. • Belgelendirme denetimi sürecinin yönetimi.	• Daha önce birçok bilgi güvenliği ve sistem yönetimi projesinde liderlik deneyimi bulunmaktadır. • ISO 27001 standardı üzerine teorik ve uygulamalı bilgiye sahiptir.
Satın Alma Ahmet Emin BALCI	% 10	• Proje kapsamında gerekli ekipman ve hizmetlerin satın alma süreçlerinin yönetimi. • Tedarikçi ilişkilerinin koordine edilmesi.	• Organizasyonel tedarik zinciri yönetiminde deneyim sahibidir. • Daha önceki projelerde bilgi güvenliği altyapısı için gerekli cihaz ve yazılım tedarik süreçlerini yönetmiştir.
İnsan Kaynakları Ahmet Can ŞAHİN	% 10	• Çalışan farkındalık eğitimlerinin planlanması ve uygulanması. • Eğitim programlarının takibi ve sonuçların değerlendirilmesi.	• Çalışan eğitim ve farkındalık süreçlerinde deneyimlidir. • İnsan kaynakları yönetiminde geniş bilgiye sahiptir.
Kalite Güvence	% 20	• Proje süreçlerinin kalite standartlarına uygunluğunu	• ISO standartları üzerine deneyim sahibidir.

Enver YAMAN		denetleme. • İç denetimlerin planlanması ve raporlanması. • Süreçlerin iyileştirilmesine yönelik öneriler geliştirme.	• Kalite yönetim sistemleri kurulumunda ve sürdürülebilirlik süreçlerinde görev almıştır.
Risk Yönetimi İsmail KARŞIĞA	% 20	• Bilgi güvenliği risklerinin değerlendirilmesi ve risk azaltma stratejilerinin geliştirilmesi. • Risk yönetim planının hazırlanması ve uygulanması.	• Kurumsal risk yönetimi ve kriz yönetimi süreçlerinde deneyimlidir. • Risk değerlendirme ve uyum süreçlerinde aktif rol almıştır.

Projenin Birim Özellikleri

- **Yönetim / Sponsor:** Proje için finansal ve idari destek sunar, genel vizyon ve hedeflerin gerçekleşmesini denetler.
- **Bilgi Teknolojileri:** Projenin teknik altyapısını sağlar, bilgi işlem süreçlerini yönetir.
- **Satın Alma:** Gerekli ekipman ve hizmetlerin tedarik edilmesini sağlar.
- **İnsan Kaynakları:** Çalışan eğitimleri ve farkındalık oluşturma süreçlerinden sorumludur.
- **Kalite Güvence:** Proje süreçlerinin kalite standartlarına uygunluğunu sağlar.
- **Risk Yönetimi:** Bilgi güvenliği risklerinin yönetilmesini ve kontrol önlemlerinin geliştirilmesini sağlar.

21. BÜTÇE ve GEREKÇESİ:

GENEL BÜTÇE TABLOSU (TL)					
Katkı Kaynağı	**Makine Teçhizat (06.1 + 06.3)**	**Sarf Malzemesi (03.2)**	**Hizmet Alımı (03.5 + 3.6)**	**Seyahat (03.3)**	**TOPLAM**
BAPK'tan Talep Edilen Katkı	749,249	6,000	300,350	25,000	**1,080,599**
Varsa Destekleyen Diğer Kuruluş Katkısı	0	0	300,000	0	**300,000**
TOPLAM	**749,249**	**6,000**	**600,350**	**25,000**	**1,380,599**

BAPK'TAN TALEP EDİLEN BÜTÇE TABLOSU		
Alınması Önerilen Makine – Teçhizat		
Adı / Modeli	**Kullanım Gerekçesi**	**Bedeli (TL)**
QNAP TS-873A NAS Storage	Bilgi güvenliği sistemleri için yedekleme ve veri depolama ihtiyaçlarını karşılamak.	60,749
Epson WF-C5790DWF Yazıcı	Kimlik doğrulama ile belge güvenliğini kaynağında sağlamak için.	15,000
Veeam Veri Yedekleme Yazılımı (Yıllık)	Server ve Client kritik verilerinin yedeklenmesi için.	20,000

Aruba Clearpass NAC Çözümü (Yıllık)	Network yetkisiz erişimleri engellemek için	175,000 (5,000 $)
Yönetilebilir L3 Switch	NAC uygulanırken kontrolleri sağlayabilecek yetenekler için.	15,000
Trellix DLP Yazılımı Veri Sızıntısı Önleme (Yıllık)	Şirket verilerinin istenmeyen hedeflere aktarılmasını engellemek, ISO27001	157,500 (4,500 $)
Disaster Recovery Disk Alanı Hizmeti (Yıllık)	Backupların veri güvenliğini sağlamak amacı ile farklı lokasyonda yedeklenmesi için.	25,000
5651 Loglama ve Hot Spot Çözümü (Yıllık)	Kullanıcı MAC Adreslerini, IP adreslerini ve WI-FI internet çıkışları imzalama yazılımı	15,000
PAM Çözümü (Yıllık) (Privileged Access Management)	Kullanıcı yetki ve Parola yönetimi için (Active Directory destek amacıyla ve kritik bir uygulamaya kimlik doğrulama yapmak için)	40,000
İşletim Sistemi ve program Patch yönetim Çözümü	İşletim Sistemleri ve programların güncelliğini koruyabilmek için yama yönetim yazılımı	25,000
XDR Özellikli Antivirus Yazılımı (Yıllık)	Şirketteki tüm PC, Server ve verileri virüs, trojan vb. korumak için.	35,000
MDM Çözümü (Yıllık) (Mobile Device Management)	Firmaya ait olup firma dışında kullanılan cihazların yönetimi için.	20,000
Lisans ve Envanter yönetim Çözümü (Yıllık)	Dijital lisansların ve firma envanterinin yönetimi için.	15,000
PDKS Sistemi	Yetkisiz erişimleri önlemek için.	45,000
Kamera Kayıt Sistemi	Erişim yönetiminin takibi ve yetkisiz erişimlerin takibi için.	30,000
SIEM Çözümü (Yıllık)	Oluşan logların değerlendirilmesi ve doğru aksiyonların alınması için.	50,000
Kilitli Özlük Dosyası Dolabı	Kritik personel verilerini güvenli bir şekilde saklamak için.	6,000
TOPLAM		749,249

Alınması Önerilen Sarf Malzemesi		
Adı	**Kullanım Gerekçesi**	**Bedeli (TL)**
A4 Kağıt (5 Koli)	Dokümantasyon çıktıları ve eğitim materyalleri için.	2,500
Toner (3 Adet)	Yazıcı çıktılarının alınması için.	1,500
Klasör ve Dosya Seti	ISO 27001 dokümanlarının düzenlenmesi ve arşivlenmesi için.	1,000
Etiket ve Post-it	Dosya yönetimi ve doküman işaretlemeleri için.	500
Diğer Ofis Malzemeleri	(Kalem, yapışkan, zımba vb.) Proje çıktılarının düzenlenmesi ve çalışanların kullanımı için.	500

TOPLAM		6,000

(KDV dahil bedeli yazılmalıdır.)

Hizmet Alımı		
Mahiyeti	**Gerekçesi**	**Bedeli (TL)**
ISO 27001 Belgelendirme Hizmeti	Uluslararası akreditasyona sahip bir kuruluş tarafından dış denetim yapılması.	87,500
Danışmanlık Hizmeti	Risk değerlendirme, dokümantasyon ve eğitim süreçlerinde uzman desteği alınması.	162,500
Penetrasyon Testi (Sızma Testi)	Kurumların kendi sistemlerini saldırgan bakış açısı test ederek veya ettirerek sistemlerinin güvenli olup olmadığını öğrenmek için	350,000 (10,000 $)
Alan Adı ve Mail SSL Sertifikası (Yıllık)	Web sayfası, maillere ve CRM sistemine web üzerinden erişim güvenliği için.	350
TOPLAM		600,350

(KDV dahil bedeli yazılmalıdır.)

Seyahat Giderleri			
Yurt içi seyahat giderleri	**Kişi Adedi**	**Gerekçe**	**Toplam (TL)**
Denetim ve Eğitim Seyahati	3	Dış denetim sırasında denetçiler için ulaşım	5,000
Denetim ve Eğitim Seyahati	3	Dış denetim sırasında denetçiler için konaklama	15,000
İç Denetim Çalışmaları	2	İç denetimlerde danışmanların proje yerine seyahati.	5,000
Yurt dışı seyahat giderleri	**Kişi Adedi**	**Gerekçe**	**Toplam (TL)**
-	0	0	0
		TOPLAM	25,000