# ISO 27001 BGYS Doküman ve Belgelendirme Süreci

## ****1. Proje Başlığı****

ISO, Uluslararası Standardizasyon Örgütünün (International Organization for Standardization) kısaltmasıdır. Bu örgüt dünya genelinde kabul görmüş standartların geliştirilmesi ve teşvik edilmesinden sorumludur. ISO belgelendirme, bir organizasyonun belirli bir standartta tanımlanan gerekliliklere uygun olarak çalıştığını bağımsız bir denetim kuruluşu tarafından onaylama sürecidir. Bu süreç, bir kuruluşun kalite, güvenlik, çevre yönetimi veya bilgi güvenliği gibi alanlarda uluslararası kabul görmüş kriterlere uygun şekilde çalıştığını tescil eder.

ISO belgelendirme, kuruluşlara birçok avantaj sağlar. Öncelikle, iş süreçlerini düzenleyerek verimliliği artırır. Ayrıca, müşterilere ve iş ortaklarına güven verir, çünkü bir ISO sertifikası, organizasyonun işleyişinin sistematik ve şeffaf olduğunu gösterir. Bunun yanı sıra, yasal düzenlemelere uyum sağlamayı kolaylaştırır ve uluslararası pazarda rekabet avantajı sunar.

ISO standartlarının en temel prensiplerinden biri olan “Yazdığını yap, yaptığını yaz” anlayışı, süreçlerin hem dokümantasyonla tanımlanmasını hem de bu dokümantasyonlara uygun şekilde uygulanmasını gerektirir. Bu yaklaşım, hem şeffaflığı artırır hem de organizasyon içindeki süreçlerin izlenebilirliğini sağlar.

## ****2. Önerilen Proje Süresi, Toplam Bütçe ve Destek Miktarı****

Bu proje için önerilen toplam süre 12 aydır. Bu süre, projenin kapsamı ve hedefleri göz önünde bulundurularak belirlenmiştir. Her bir aşama, GAP Analizi, Eğitim, Risk Yönetimi, Dokümantasyon, Kontrol ve Belgelendirme gibi bölümler halinde planlanmıştır ve bu aşamalar için gereken süre detaylı bir şekilde hesaplanmıştır. 12 aylık süre zarfında, proje ekibi her bir adımı zamanında ve etkin bir şekilde tamamlamayı hedeflemiştir.

Projenin toplam bütçesi 1,380,599 TL olarak belirlenmiştir. Bu bütçe, gerekli ekipman, hizmet alımları, seyahat ve sarf malzemesi giderlerini kapsamaktadır. Ayrıca, bütçenin bir kısmı, belgelendirme ve danışmanlık gibi uzmanlık gerektiren süreçlerde kullanılacaktır.

Bu proje için farklı kurumlar destek sağlamaktadır. **Enderun Akademi ISO 27001 danışmanı olarak, KIWA** TÜRKAK akreditasyonlu belgelendirme kuruluşu olarak denetim ve sertifikasyon süreçlerini üstlenmiştir. Nebula Bilişim, Penetrasyon Testi (Sızma), DLP için Veri Sınıflandırma ve Varlık Tespiti Danışmanlık Hizmeti, Spam ve Phishing Farkındalık Eğitimi desteği alınmıştır. Ayrıca, 2024 yılı itibarıyla KOSGEB tarafından sağlanan finansal destek, projenin bir kısmını karşılamıştır. KOSGEB desteğinin üst limiti 300,000 TL olup destek oranı proje bedelinin %60 ı kadardır.

## ****Proje Ekibi****

* **Sedat ÖZTÜRK (Proje Yöneticisi):** Bilgi Teknolojileri alanında uzman olan Sedat ÖZTÜRK, projenin genel koordinasyonundan ve ekipler arası iletişimin sağlanmasından sorumludur.
* **Ömer ENDEN (Danışman):** ISO 27001 süreçlerinde deneyimli bir uzman olan Ömer ENDEN, risk yönetimi, dokümantasyon ve eğitim süreçlerinde teknik rehberlik sağlamaktadır.
* **Ahmet Emin BALCI (Satın Alma Sorumlusu):** Projede ihtiyaç duyulan ekipman ve hizmetlerin tedarik sürecini yöneterek, kaynakların etkin kullanımını sağlamaktadır.
* **Ahmet Can ŞAHİN (İnsan Kaynakları Sorumlusu):** Çalışan farkındalık eğitimlerinin planlanması ve uygulanmasından sorumludur.
* **İsmail KARŞIĞA (Risk Yönetimi Sorumlusu):** Bilgi güvenliği risklerinin analiz edilmesi ve yönetilmesinde lider rol oynamaktadır.
* **Enver YAMAN (Kalite Güvence Sorumlusu):** Projenin kalite standartlarına uygun şekilde yürütülmesini denetlemektedir.

## ****Proje Özeti****

Bilgi güvenliği, dijital çağda her organizasyon için temel bir gereklilik haline gelmiştir. Bilgi varlıklarının korunması, yalnızca iş sürekliliği açısından değil, aynı zamanda müşteri güveni ve yasal uyum açısından da önemlidir. ISO 27001 standardı, bilgi güvenliğini sistematik ve sürdürülebilir bir şekilde yönetmek için uluslararası çapta kabul görmüş bir çerçeve sunar. Bu proje, bir organizasyonun bilgi güvenliği risklerini yönetmesini, uluslararası standartlara uyum sağlamasını ve kurumsal güvenlik kültürünü güçlendirmesini hedefler. Günümüzde siber saldırıların artışı, işletmeleri daha dirençli bir güvenlik altyapısı oluşturmaya zorlamaktadır. Projenin en temel amacı, ISO 27001 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) oluşturarak, kurumun bilgi güvenliği süreçlerini optimize etmektir. Süreç boyunca çalışanların farkındalığını artırmak, dokümantasyon ve uygulamaları standartlara uygun hale getirmek öncelikli hedeftir. Projenin tamamlanmasıyla birlikte, kuruluşun bilgi güvenliği alanındaki yetkinlikleri uluslararası düzeyde tescillenecektir.

Bu proje, ISO 27001 standardına uygun bir Bilgi Güvenliği Yönetim Sistemi (BGYS) kurarak organizasyonun bilgi varlıklarını koruma ve iş sürekliliğini sağlama hedefini taşımaktadır. Proje, bilgi güvenliği süreçlerini uluslararası standartlarla uyumlu hale getirerek, yasal düzenlemelere uygunluk sağlamayı amaçlamaktadır. GAP analiziyle mevcut süreçler değerlendirilmiş ve eksiklikler belirlenmiştir. Risk yönetimi aşamasında, bilgi varlıkları detaylı bir şekilde analiz edilmiş ve olası tehditler önceliklendirilmiştir. Çalışan farkındalığı eğitimleri ile bilgi güvenliği bilinci artırılmıştır. ISO 27001'e uygun dokümantasyon hazırlanmış, tüm süreçler standartlara entegre edilmiştir. İç denetim ve belgelendirme sürecinin ardından organizasyon, ISO 27001 sertifikasını alarak bilgi güvenliği konusundaki yetkinliğini kanıtlamıştır. Proje, aynı zamanda sürdürülebilir bir bilgi güvenliği altyapısının oluşturulmasına da odaklanmıştır. Elde edilen sonuçlar, organizasyonun uluslararası pazardaki konumunu güçlendirecek ve müşteri güvenini artıracaktır.

## ****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. Proje kapsamında, firmanın uluslararası geçerliliğe sahip ve TÜRKAK akreditasyonlu bir belgelendirme kuruluşu tarafından denetlenmesi sonucunda ISO/IEC 27001:2022 BGYS belgesinin kazandırılması öngörülmektedir.

## ****Konu ve Kapsam****

Proje, organizasyonların bilgi güvenliği süreçlerini uluslararası standartlara uygun hale getirmeyi hedeflemektedir. Kapsam, organizasyonun tüm bilgi varlıklarını (elektronik, yazılı ve sözlü) korumayı içerir. Ayrıca, organizasyon genelinde tüm çalışanlar, sözleşmeli personel, alt yükleniciler ve kullanılan cihazlar bu kapsam dahilindedir. Proje, bilginin gizliliğini, bütünlüğünü ve erişilebilirliğini sağlayarak güvenlik risklerini en aza indirmeyi amaçlamaktadır.

|  |  |
| --- | --- |
| **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. |

Kapsam genişliği, proje çıktılarının yalnızca mevcut durumu değil, gelecekteki süreçleri de kapsamasını sağlamaktadır.

## ****Literatür Özeti****

Organizasyonel Kazanımlar konusunda Thomas R. Peltier (2016), kitabında bilgi güvenliği yönetiminin iş hedeflerini destekleyecek şekilde entegre edilmesi gerektiğini vurgular. Etkili bir bilgi güvenliği programı, bilgi varlıklarını korurken iş hedeflerine ulaşmayı kolaylaştırır.

Uyum ve Yasal Gereklilikler konusunda Prof. Edward Humphreys ISO 27001’in GDPR gibi veri koruma düzenlemeleriyle uyumda kritik bir rol oynadığını belirtir. Standart, kişisel veri koruma gerekliliklerini karşılamada organizasyonlara rehberlik eder ve yasal risklerin azaltılmasını sağlar.

Literatürdeki Boşluklar 3 başlıkta değerlendirilmiştir.

Kurumlara Özel Uyarlamalar ISO 27001’in farklı organizasyonlara uygulanması konusunda genel bilgiler sunsa da, kuruma özel uygulamalar yeterince ele alınmamıştır. Areej AlHogail (2018), kuruma özgü BGYS tasarımlarının ve risk değerlendirme yöntemlerinin geliştirilmesinin önemini vurgular.

Süreçlerin Sürdürülebilirliği konusunda ISO 27001 sistemlerinin sürdürülebilir yönetimi hakkında yeterince çalışma yapılmamıştır. Siponen & Willison (2009), sürekli eğitim, performans değerlendirme ve iç denetim süreçlerinin eksikliğine dikkat çekmiştir.

Çalışan Farkındalığı kısmında bilgi güvenliği farkındalığı üzerine yapılan çalışmalar sınırlıdır. Kritzinger & Smith (2008), bilgi güvenliği farkındalığının artırılması için daha etkin eğitim yöntemlerine ihtiyaç duyulduğunu belirtir.

## ****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.

ISO 27001, bilgi güvenliği yönetimini hem teknik hem de yönetsel süreçlerle ele almaktadır. Literatürde, ISO 27001’in özellikle GDPR gibi yasal düzenlemelerle uyum sağlamada kritik bir araç olduğu vurgulanmıştır. Ancak, sektörel adaptasyon ve sürdürülebilirlik konularında yeterince çalışma bulunmamaktadır. Bu proje, bu boşluğu doldurarak, sektörel farklılıkları ve uzun vadeli sürdürülebilirlik mekanizmalarını araştırmıştır. Proje çıktıları, literatürdeki bu eksikliklere doğrudan katkı sağlayacak şekilde yapılandırılmıştır.

## ****Yöntem****

Proje, üç temel yöntemle ilerlemiştir: dokümantasyon, eğitim ve belgelendirme. Dokümantasyon sürecinde, ISO 27001 gerekliliklerine uygun prosedürler ve politikalar hazırlanmıştır. Eğitim aşamasında, çalışanlara farkındalık kazandırılmış ve teknik ekip iç denetim süreçleri konusunda eğitilmiştir. Belgelendirme aşamasında ise, iç denetimlerin ardından uluslararası akreditasyona sahip bir kuruluş tarafından yapılan dış denetimlerle süreç tamamlanmıştır.

## ****Araştırma Olanakları****

Projede, mevcut bilgi işlem altyapısı, ağ sistemleri, sunucu altyapısı, Bimser (QDMS) yazılımlar etkin bir şekilde kullanılmıştır. Eğitimler için görsel-işitsel araçlar ve interaktif modüller hazırlanmıştır. Ayrıca, bilgi güvenliği uzmanlarından danışmanlık hizmetleri alınarak süreçler desteklenmiştir.

|  |  |
| --- | --- |
| **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. |

## ****Yaygın Etki ve Katma Değer****

Proje, ulusal ekonomiye ve organizasyonel süreçlere önemli bir katkı sağlamaktadır. ISO 27001 standardı, organizasyona uluslararası pazarda rekabet avantajı sunmuş ve müşteri güvenini artırmıştır. Ayrıca, bilgi güvenliği farkındalığını toplumsal düzeyde artırarak bireylerin dijital güvenliğini desteklemiştir. Proje çıktıları, bilgi güvenliği alanında bilimsel birikime katkıda bulunarak, sektörel uyarlamalara yönelik yeni bir model sunmuştur.

## ****Çalışma Takvimi****

Proje, 12 aylık bir takvim çerçevesinde yürütülmüştür. İlk iki ay proje açılışı ve ekip ataması gerçekleştirilmiştir. 3. ve 4. aylarda GAP analizi yapılmış, eksiklikler raporlanmıştır. 5. ve 6. aylarda eğitim faaliyetleri tamamlanmış, 9. ve 10. aylarda dokümantasyon süreçleri sonuçlandırılmıştır. 11. ayda iç denetimler yapılmış ve 12. ayda sertifikasyon süreci başarıyla tamamlanmıştır. Bu takvim, projenin sistematik bir şekilde ilerlemesini sağlamıştır.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **İş Paketi Ad/Tanım** | | **AYLAR** | | | | | | | | | | | |
| **1** | **2** | **3** | **4** | **5** | **6** | **7** | **8** | **9** | **10** | **11** | **12** |
| **1** | **Proje Açılışı**   * **Proje Tanıtımı**: Projenin hedefleri, kapsamı ve önemi tüm paydaşlara açıklanır. Bilgi güvenliği yönetim sistemi oluşturma sürecinin gerekliliği ve sağlayacağı faydalar vurgulanır.(Kapsam ve Hedefler BGYS El Kitabı) * **Proje Ekibinin Atanması**: Alanında uzman ekip üyeleri seçilir ve görev dağılımları yapılır. Ekip, bilgi güvenliği yönetiminde ihtiyaç duyulan beceri ve deneyimlere sahip bireylerden oluşur. * **BG Ekibinin Ataması**: Bilgi Güvenliği Ekibi, projeye özel olarak atanır ve tüm süreçlerin yürütülmesinde aktif rol oynar. Bu ekip, özellikle dokümantasyon, risk yönetimi ve denetim süreçlerini yönlendirir. |  |  |  |  |  |  |  |  |  |  |  |  |
| **2** | **GAP Analizi**   * **Mevcut Durum Tespiti**: Organizasyonun mevcut bilgi güvenliği süreçleri, politikaları ve uygulamaları analiz edilir. Eksikliklerin ve zayıf noktaların belirlenmesi için detaylı bir inceleme yapılır. (Tehditler, Zayıflıklar, Risk Yönetimi) * **Boşluk Analizi**: ISO 27001 gereklilikleriyle mevcut durum karşılaştırılarak eksiklikler belirlenir. Bu analiz, organizasyonun risklerini ve iyileştirme ihtiyaçlarını açıkça ortaya koyar. (BGYS Politikalar El Kitabı) * **Raporlama**: Analiz sonuçları raporlanır ve hangi alanlarda gelişim sağlanması gerektiği belirtilir. Bu rapor, projenin sonraki aşamalarında bir rehber olarak kullanılır. |  |  |  |  |  |  |  |  |  |  |  |  |
| **3** | **Eğitim**   * **Farkındalık Eğitimi**: Tüm çalışanlara bilgi güvenliğinin önemi ve ISO 27001 standartları hakkında temel bilgiler verilir. Eğitim, organizasyonda ortak bir güvenlik bilinci oluşturmayı amaçlar. (Egitim\_Plani) * **ISO 27001 Standart Eğitimi**: Teknik ekip ve yöneticilere, standardın gereklilikleri ve uygulamaları hakkında detaylı bilgi sunulur. Eğitim, teorik bilgiler ile pratik uygulamaları birleştirir. * **ISO 27001 İç Denetçi Eğitimi**: Denetim süreçlerini yönetecek ekipler, iç denetim prosedürlerini ve kontrol mekanizmalarını öğrenir. Bu eğitim, belgelendirme sürecinde iç denetimlerin etkinliğini artırır. |  |  |  |  |  |  |  |  |  |  |  |  |
| 4 | **Risk Yönetimi**   * **Varlık Envanterinin Hazırlanması:** Organizasyonun bilgi varlıkları, sistematik bir şekilde tanımlanır ve sınıflandırılır. Bu liste, risk analizinin temelini oluşturur. (Varlık Envanteri) * **Risk Envanterinin Hazırlanması:** Her varlık için olası tehditler ve zayıflıklar belirlenir. Tehditlerin olasılık ve etkileri değerlendirilerek riskler sıralanır. * **Risk Analizi:** Belirlenen riskler, "Olasılık × Etki" formülüyle önceliklendirilir. Kritik riskler için azaltıcı veya önleyici kontroller geliştirilir. (Risk Yönetimi) |  |  |  |  |  |  |  |  |  |  |  |  |
| **5** | **Dokümantasyon**   * **ISO 27001 El Kitabı:** Organizasyonun bilgi güvenliği yönetim sistemine genel bir rehberlik sağlar. * **ISO 27001 BG Politikaları:** Bilgi güvenliği süreçlerini destekleyen politikalar hazırlanır ve dokümante edilir. * **Uygulanabilirlik Bildirgesi (SoA):** Uygulanan ve uygulanmayan kontroller listelenir; gerekçeleri açıklanır. (Uygulanabilir Bildirgesi) * **İş Sürekliliği Planı:** Olası bir aksaklık durumunda operasyonların devamlılığını sağlamak için planlar geliştirilir. (İş Sürekliliği Talimatı) * **ISO 27001 BG Prosedürleri:** Sistematik süreçleri destekleyen prosedürler yazılır. |  |  |  |  |  |  |  |  |  |  |  |  |
| 6 | **Kontrol**   * **İç Denetim:** Sistem, ISO 27001 standartlarına uygunluk açısından değerlendirilir. Bu denetimler, eksikliklerin tespit edilmesine yardımcı olur. * **Düzeltici Faaliyetler:** İç denetimlerde tespit edilen uygunsuzluklar giderilir. Bu faaliyetler, sistemin performansını artırır. ( * **Yönetimi Gözden Geçirme:** Üst yönetim, sistemin genel performansını değerlendirir ve stratejik iyileştirme kararları alır. |  |  |  |  |  |  |  |  |  |  |  |  |
| 7 | **Belgelendirme**   * **1. Aşama Denetim:** Dokümantasyon ve temel süreçler denetlenir. Sistem, ISO 27001 gerekliliklerine uygunluk açısından değerlendirilir. * **2. Aşama Denetimi:** Uygulama süreçleri, kontrollerin etkinliği ve çalışan farkındalığı denetlenir. Yerinde yapılan bu denetimler, belgelendirme sürecinin en kritik adımıdır. |  |  |  |  |  |  |  |  |  |  |  |  |

## ****Başarı Ölçütleri****

Projenin başarıya ulaşması için çeşitli ölçütler belirlenmiştir. Risk yönetiminde bilgi varlıklarının detaylı bir envanteri çıkarılmış, tehditler analiz edilmiştir. Dokümantasyonun standartlara uygunluğu ve organizasyonel süreçlerle entegrasyonu sağlanmıştır. Eğitimlerin etkinliği, çalışan farkındalığını ölçen testlerle değerlendirilmiştir. Son olarak, ISO 27001 sertifikasının alınması, projenin en somut başarı ölçütü olmuştur.

* **B Planı:** Projede olası aksaklıklar için alternatif stratejiler geliştirilmiştir. GAP analizi veya risk yönetiminde eksiklikler tespit edilirse, harici danışmanlardan destek alınması planlanmıştır. Eğitimlerde düşük katılım oranlarına karşı çevrimiçi platformlar devreye sokulmuştur. Dokümantasyon sürecinde, eksiklikler hızlıca tamamlanmak üzere sadeleştirilmiştir. Bu alternatifler, proje çıktılarının zamanında ve eksiksiz şekilde elde edilmesini sağlamıştır.

## ****Görev Dağılımı****

Görevler, ekip üyelerinin uzmanlık alanlarına uygun şekilde dağıtılmıştır. Proje yöneticisi genel koordinasyonu sağlarken, danışman teknik rehberlik sunmuştur. Satın alma, eğitim, kalite güvence ve risk yönetimi ekiplerinin her biri, projenin belirli bir aşamasından sorumlu olmuştur. Bu görev dağılımı, işlerin hızlı ve verimli bir şekilde tamamlanmasını sağlamıştır. Ayrıca, her üyenin katkısı, proje çıktılarının kalitesini artırmıştır.

## ****Bütçe ve Gerekçesi****

Projenin toplam bütçesi 1,380,599 TL olarak belirlenmiştir. Bu bütçe, ekipman, sarf malzemesi, hizmet alımı ve seyahat giderlerini kapsamaktadır. Ayrıca, belgelendirme ve danışmanlık gibi uzmanlık gerektiren süreçler için de kaynak ayrılmıştır. Bütçe planlaması, kaynakların etkin kullanımı ve sürdürülebilirliğini sağlamak amacıyla yapılmıştır. Destekleyici kurumların katkıları, bütçenin dengeli bir şekilde dağıtılmasını sağlamıştır. Ek giderler, özellikle bilgi güvenliği sisteminin altyapısını güçlendirmek için ayrılmıştır. QNAP NAS Storage, FortiGate güvenlik sistemleri ve Trellix DLP yazılımı gibi teknolojiler için bütçe planlanmıştır. Ayrıca, sertifikasyon sürecinde kullanılmak üzere danışmanlık ve eğitim giderleri de eklenmiştir. Bu giderler, organizasyonun bilgi güvenliği altyapısını modernize etmek ve sürdürülebilirlik sağlamak için kritik öneme sahiptir. Ek giderler, projenin genel başarısına önemli bir katkı sağlamıştır.