T.C. İçişleri Bakanlığı Göç İdaresi Genel Müdürlüğü
GöçNet Projesi
Bilişim Sistemleri Denetimi Özeti

Giriş

19.07.2016 tarihinde Resmi Gazete'de yayımlanarak yürürlüğe giren 2016-2019 Ulusal e-Devlet Stratejisi ve Eylem Planı ile "Kamuda e-Devlet Projelerinin Etkin Denetiminin Sağlanması" eylemi Sayıştayın sorumluluğuna verilmiştir. Bu kapsamda, "e-Devlet Projeleri Denetim Modeli" ve "e-Devlet Projeleri Denetim Rehberi (Taslak)" hazırlanmış ve T.C. İçişleri Bakanlığı Göç İdaresi Genel Müdürlüğü (GİGM) bünyesinde yürütülen GöçNet Projesinin pilot denetiminin yapılması kararlaştırılmıştır.

Proje Hakkında Bilgi

GöçNet Projesi, yabancılara ait iş ve işlemlerin elektronik ortama taşınmasını, ilgili kurum ve kuruluşlar ile bilgi akışının entegre şekilde çalışmasını sağlamak amacıyla oluşturulmuş bir projedir.

2013 yılı içerisinde başlanan ve 2015 yılı Mayıs ayı itibarıyla, GİGM merkez ve taşra birimlerinde kullanımına başlanan GöçNet Kurumsal Bilişim Projesi; 46 fiziksel, 210 sanal sunucu ile kapalı devre olarak Genel Müdürlük merkez teşkilatı, 81 İl Göç İdaresi Müdürlüğü, 14 İlçe Grup Başkanlığı ve 20 Geri Gönderme, Kabul ve Barınma Merkezinde hizmet veren bir yapıdadır.

GöçNet e-Devlet Uygulaması; 17 farklı modül üzerinde kapalı devre olarak çalışan bir proje olarak tasarlanmıştır. Ayrıca IP Sec VPN, noktadan noktaya ve KamuNet bağlantıları üzerinden çok sayıda kamu kurum ve kuruluşlarının bilgi sistemleri ile entegre olarak çalışmaktadır.

Denetimin Amacı ve Metodolojisi

GöçNet Projesi pilot denetimi kapsamında;

- Projenin kendisinin ve yürütüldüğü bilişim ortamının gizlilik, bütünlük, erişilebilirlik, güvenilirlik, verimlilik, etkililik ve mevzuata uygunluğunu sağlamaya yönelik bilişim teknolojileri (BT) kontrollerinin incelenmesi,
- Projenin başarı ile tamamlanmasını engelleyebilecek sorunların tespit edilmesi ve gerekli önlemlerin alınması için öneri sunulması yoluyla kuruma katkı sağlanması,
- Raporlama yolu ile ilgililerine Proje hakkında bilgi sunulması

hedeflenmiştir.

GöçNet projesinin denetiminde; COBIT (Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri), ITAF (Bilgi Teknolojileri Güvence Çerçevesi), PMBOK (Proje Yönetimi Bilgi Birikimi) Kılavuzu ve ISO/IEC 27000 Standart Serisi ile Uluslararası Yüksek Denetim Kurumları Standartları (ISSAI) esas alınarak hazırlanmış olan e-Devlet Projeleri Denetim Rehberinde (Taslak) belirlenen metodoloji takip edilmiştir.

Bu çerçevede; risk tabanlı denetim yaklaşımına uygun olan ve aşağıda belirtilen denetim yaklaşımı izlenmiştir:

1. GöçNet Projesinin kendisine ve yürütüldüğü bilişim ortamına ilişkin risklerin belirlenmesi,
2. Bu riskleri minimize edebilecek kontrollerin belirlenmesi,
3. Bu kontrollerin GİGM tarafından oluşturulup oluşturulmadığı, eğer oluşturulmuş ise etkin çalışıp çalışmadığının incelenmesi,
4. İnceleme sonucu tespit edilen kontrol zafiyetlerinin değerlendirilmesi ve
5. Denetim sonucunda, önemli görülen kontrol zafiyetlerinin raporlanarak ilgililerine sunulması.

Projenin kendisi yanında, geliştirildiği Kurum bilişim ortamı ve altyapısı (sunucular, ağ, veri tabanları) ile uygulamanın hizmete sunulduğu web yapıları da denetime ve denetime özgü testlere konu edilmiştir.

GöçNet e-Devlet uygulamasının tüm modülleri uygulama kontrollerine tabi tutulmamış olup, uygulama kontrollerinin hangi modüller üzerinde test edileceğinin belirlenmesi için;

- Önemlilik (Uygulamanın kurum faaliyetlerine ve mali tablolara etkisi vs.),
- Kritiklik (Kurumsal bilgilerin bütünlüğü, gizliliği ve erişilebilirliği vs.),
- Karmaşıklık (Kullanıcı sayısı, işlem hacmi, vs.),

- Teknolojik Altyapı (İşletim sistemi, yazılım geliştirme ortamı, veri tabanı vs.),
- Kontrol Çevresi (Destek personeli, dokümantasyonu, karşılaşılan hatalar vs.),

gibi hususları ve denetim kaynaklarını da dikkate alınarak, denetim ekibi değerlendirmesi sonucunda tespit edilen modüller uygulama kontrolleri açısından ayrıntılı olarak incelenmiştir.

Denetimde Taslak Rehberdeki kontrol alanlarında yer alan kontrollerin varlık, tasarım ve işleyiş etkinliği değerlendirilmiştir. Bu çerçevede,

BT Yönetişim Kontrolleri kapsamında; "BT Stratejisi", "Politika ve Prosedürler", "Organizasyon, Rol ve Sorumluluklar", "İnsan Kaynakları ve Eğitim", "Gereksinim Tanımlama", "Yasal ve Diğer Düzenlemelere Uygunluk", "Risk Değerlendirme" ve "Varlık Yönetimi",

Proje Yönetimi Kontrolleri kapsamında; "Proje Öncesi Çalışmalar" "Entegrasyon Yönetimi", "Kapsam Yönetimi", "Zaman Yönetimi", "Bütçe Yönetimi", "Kalite Yönetimi", "İnsan Kaynakları Yönetimi", "İletişim Yönetimi", "Risk Yönetimi" ve "Paydaş Yönetimi",

Dış Tedarik Kontrolleri kapsamında; "İhale Süreci", "Sözleşme Uygulama Süreci" ve "Muayene ve Kabul",

Bilgi Güvenliği Kontrolleri kapsamında; "Sistem Güvenlik Gereksinimleri Tasarımı", "Fiziksel ve Çevresel Güvenlik", "Ağ Güvenliği", "İşletim Sistemi Güvenliği", "Veri Tabanı Güvenliği", "Web Uygulama Güvenliği" ve "Mobil Uygulama Güvenliği",

İşletim ve Bakım Yönetimi Kontrolleri kapsamında; "Hizmet Seviyesi Yönetimi", "Konfigürasyon Yönetimi", "Olay ve Problem Yönetimi", "Değişim Yönetimi" ve "Kapasite Yönetimi",

İş Sürekliliği ve Felaket Kurtarma Planlaması Kontrolleri kapsamında; "İş Sürekliliği Organizasyonu", "Risk Değerlendirmesi", "İş Etki Analizi", "İş Süreklilik Planı", "Felaket Kurtarma Planı", "Belgelendirme", "Test ve Güncelleme" ve "Yedekleme",

Uygulama Kontrolleri kapsamında; "Girdi", "Veri Transferi", "İşlem" ve "Çıktı",

Proje İçerik ve Süreç Kontrolleri kapsamında; "Planlama", "Tasarım", "Kod Geliştirme", "Test", "Kabul ve Kurulum", "Paralel Çalıştırma ve İzleme" ve "Veri Aktarımı"

alt alanlarına ilişkin kontroller incelenmiştir.

Projenin değerlendirilmesi sonucunda tespit edilen kontrol zafiyetleri; ilgili olduğu kontrol alanı, ilişkilendirildiği denetim kriteri, taşıdığı risk düzeyi, ilgili olduğu mevzuat ve/veya standartlar ile olası etkilerini içerecek şekilde açıklanmıştır.

Bu şekilde hazırlanan Taslak Rapor, bulgular hakkında görüşü alınmak üzere denetlenen Kurum ile paylaşılmış olup, Kurum görüşü dikkate alınarak Rapora son hali verilmiştir.

Raporda belirtilen hususlara yönelik olarak izleme faaliyetleri gerçekleştirilecektir. İzleme faaliyetlerinin hangi sıklıkla ve ne zaman yapılacağı ayrıca planlanacaktır.