T.C. Sağlık Bakanlığı
e-Nabız 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. Sağlık Bakanlığı bünyesinde yürütülen e-Nabız Projesinin pilot denetiminin yapılması kararlaştırılmıştır.

Proje Hakkında Bilgi

Ulusal Sağlık Sistemi (USS); sağlık politikaları oluşturulması ve sağlık hizmet kalitesinin artırılması amacıyla Sağlık Bakanlığı tarafından geliştirilen ve tüm sağlık kurum ve kuruluşlarında oluşturulan sağlık verilerinin web servisler aracılığıyla çevrim içi toplanmasını, işlenmesini ve veri kalitesinin yükseltilmesini amaçlayan bir kayıt sistemidir.

USS'nin bir bileşeni olan ve denetimin konusunu oluşturan e-Nabız ise; vatandaşların kendi sağlık verilerine (test-tahlil sonuçları, tıbbi görüntüler, muayene ve reçete bilgileri, vb.) internet ve mobil cihazlar üzerinden erişebilmelerini ve bunları yetkilendirdikleri yakınları ve hekimleri ile paylaşabilmelerini sağlayan ulusal kişisel sağlık kaydı uygulamasıdır.

e-Nabız üzerinden ayrıca; kan, kemik iliği ve organ bağışı yapılabilmekte, ziyaret edilen sağlık tesisleri değerlendirilebilmekte, sağlık tesislerinden randevu alınabilmekte, ilaçların prospektüs bilgisi ve kutu resimleri görülebilmektedir. Bunun yanında, e-Nabız mobil uygulaması kullanılarak; 112 Acil Komuta Merkezi ile iletişime geçilebilmekte, mobil sağlık uygulamalarından ve giyilebilir sağlık araçlarından alınan veriler kişisel sağlık kayıtlarına eklenebilmektedir.

Sağlık Bakanlığı ile Türksat Uydu Haberleşme Kablo TV ve İşletme A.Ş. arasında Eylül 2016'da 24 ay süreli "Ulusal Sağlık Sisteminin Bakım, Onarım, Geliştirme, Teknik Destek Hizmetlerinin Verilmesi ve Diğer Kurumsal Uygulamalara Entegrasyon İşleri Hizmet Alımı Sözleşmesi" imzalanmıştır. Denetim, yukarıda değinilen sözleşme uyarınca yürütülen ve

kapsamında e-Nabız'ın da yer aldığı yazılım modernizasyon projesi ekseninde, Ekim 2017-Mayıs 2018 arasında gerçekleştirilmiştir.

Denetimin Amacı ve Metodolojisi

e-Nabız 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.

e-Nabız 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. e-Nabız Projesinin kendisine ve yürütüldüğü bilişim ortamına ilişkin risklerin belirlenmesi,
2. Bu riskleri minimize edebilecek kontrollerin belirlenmesi,
3. Bu kontrollerin Sağlık Bakanlığı 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 ve uygulamanın kendisi yanında, geliştirildiği Kurum bilişim ortamı ve altyapısı (sunucular, ağ, veri tabanları) ile uygulamanın hizmete sunulduğu web ve mobil yapılar da denetime ve denetime özgü testlere konu edilmiştir. Toplanan sağlık verilerinin

üretildiği hastane bilgi yönetimi sistemleri ve aile hekimliği bilgi sistemleri ile sağlık verilerinin transferine ilişkin süreçler denetim kapsamı dışında bırakılmıştır.

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.