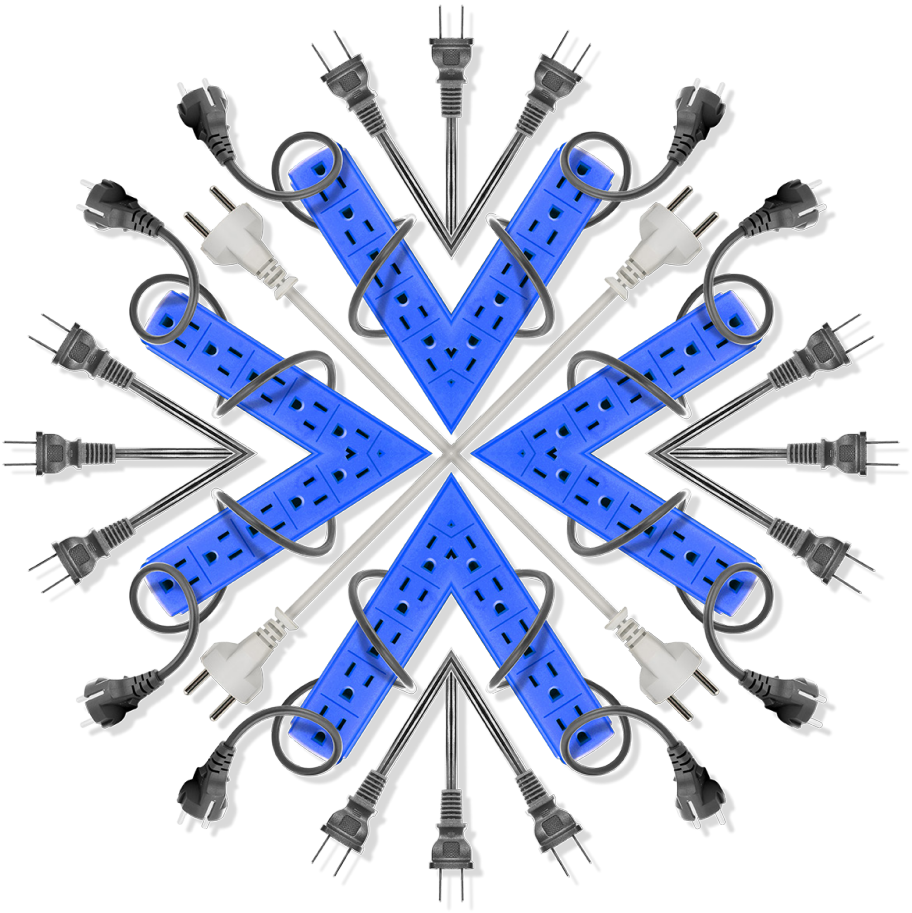

Bilgi Sistemlerinde Yeni Bir Dönem Başlıyor

Bankacılık Düzenleme ve Denetleme Kurumu tarafından **15.03.2020** tarihinde **31069** sayılı resmi gazetede yayımlanan "Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik" bilgi teknolojileri alanında yeni bir dönemin işaretçisi olmaya aday bir mevzuat olarak görülmektedir.

Yönetmelik, bankalarda teknoloji yönetiminden sorumlu olanlar ve kullanıcılar açısından yol gösterici olmakla birlikte, yalnızca bankacılık sektörünün değil, ülkenin bütününün faydalanabileceği önemli bir modeli ortaya koymaktadır.

Günümüz ve yakın geleceğin önemli tüm teknoloji noktalarına değindiği görülen Yönetmelik, yalnızca ülkemizde yayımlanan bilgi sistemleri mevzuatının birkaç adım ileri gitmesini sağlamakla kalmayıp, yaygın bilinen tüm küresel uygulama ve modellerle de uyumu kolaylaştıracak bir kılavuz niteliği taşımaktadır.

Yönetmelik'te en öne çıkan konular nelerdir diye baktığımızda pek çok önemli noktaya değindiği görülmektedir. Öncelikle, Yönetmelik'in beklediği şekilde bir teknoloji işletimini sağlamak için gerekli yönetişim yapısına değinilmesi çok değerli bir farkındalık oluşturmaktadır. Pek çok standart çerçeve veya model, iyi bir duruma gelmek için gereklilikleri açıklarken gelinen bu iyi durumda kalmayı sağlayacak mekanizmayla olan yönetişimi ya hiç ele almamaktadır ya da en son ele alınması gereken bir unsur olarak görmektedir. Bu Yönetmelik ise, en başından iyi bir yönetişim mekanizması olmadan gelinen noktada sürekliliğin sağlanamayacağı bilinciyle öncelikle bu alana yönlendirmektedir.

Günümüz koşullarında, sayısız ve her geçen gün kendini yenileyen geliştiren tehdit ve risk dünyasında, artık sınırsız ve dağınık bir şekilde önlemler almanın hem yetersiz hem de çok maliyetli hale gelmesi her konuda harekete geçmeden önce bir risk yönetimi yaklaşımı uygulanmasını zorunlu kılmaktadır. Yönetmelik de bu yaklaşıma uygun bir şekilde, Bilgi Sistemleri Risk Yönetimi sürecini ilk ele alınması gereken alan olarak açıklamaktadır. Geçmişte risk değerlendirmesinin etkin ve kapsamlı bir şekilde yapılmış olması en dikkati çeken husus iken, pek çok standardın ve modelin de katkısı ile bu konuda kurumlar pek çok deneyim yaşamıştır.

Geldiğimiz noktada ise risk yönetiminin en çok dikkat edilmesi gereken adımı değişmiş ve risklerin kabul edilmesi ve kabul edilen risklerin yönetimi en kritik noktalardan biri olmaya başlamıştır.

Yönetmelik'teki en önemli hususlardan birisi de, bilgi güvenliği fonksiyonunun Genel Müdür veya Yönetim Kurulu Üyesi'ne bağlanması gerekliliğidir. Günümüzde yalnızca bankacılıkta değil tüm sektörlerde siber tehditlerin kurumların en önemli risklerinden birisi haline gelmesi, bilgi güvenliği faaliyetlerinin en üst seviyeden takip edilmesini zorunlu kılmaktadır. Bu anlamda Yönetmelik, olması gerekli bir alanda öncü niteliği taşımaktadır.

Ülkemizde, 6698 sayılı Kişisel Veri Koruma Kanunu ile birlikte her türlü ticari işletmenin, çalışanlarının ve müşterilerinin kişisel verilerini koruması için önlemler alması ve süreçler tasarlanması ile birlikte teknoloji alanında da önemli bir gelişim noktası yakalanmıştır. Yönetmelik, kişisel veri kavramının yanı sıra hassas veri kavramı ile birlikte, yalnızca gerçek müşterilerinin değil tüzel müşterilerinin de verilerinin korunmasının önemine değinmektedir. Bu anlamda, veri korumanın bir bütün olarak ele alındığı daha ileri bir seviye için de yol göstermektedir. Ayrıca veri mahremiyeti konusunda, müşterinin açık rızasının alınması, verilecek bankacılık hizmeti için bir ön şart haline getirilememektedir.

Yönetmelik'in dikkati çeken özelliklerinden birisi de pek çok standart veya model gibi bilgi sistemlerinin sınırlı bir alanı ile ilgili olmamasıdır. Yönetmelik'te bilgi güvenliğinin yanı sıra sistem geliştirme, süreklilik ve dış hizmet alımlarına da aynı ölçüde yer verilmiştir. Sistem geliştirmenin günümüzdeki önemli aşamalarından olan bilgi mimarisi, güvenli kod geliştirme, yazılım kalitesi gibi konulara da detaylı bir şekilde değinilmektedir.

Geçmişte, bankalarda süreklilik yönetiminde en çok tartışılmış kavramlardan olan birincil ve ikincil sistemler için de Yönetmelik'te ilave açıklamalara yer verilmiştir. Bankaların kullanmakta olduğu herhangi bir sistem ya da uygulamanın birincil sistemler kapsamına girmemesi için aynı zamanda sistem veya uygulama üzerinden herhangi bir iş sürecinin yürütülmemesi, hassas veri ya da bankacılık sırrı kapsamına girebilecek verilerin işlenmemesi, iletilmemesi ve saklanmamasının gerekli olduğu ifade edilmiştir. Ayrıca, birincil sistemlerin kaçıncı yedeği olduğuna bakılmaksızın, birincil sistemlerin her türlü yedeği ikincil sistemler olarak kabul edilmektedir. Bankaların, yurt dışında kurulu bir sistemden herhangi bir onay sürecine tabi olmaksızın bankacılık işlemlerini gerçekleştirebilmesi ve yurt dışı iletişim ağlarıyla bağlantılarının kesildiği durumlarda dahi yurt içinde kurulu bulunan birincil ve ikincil sistemleri aracılığıyla ülke içerisinde bankacılık faaliyetlerini sunmaya devam edebilmesi gerekliliği açıkça belirtilmiştir.

Birincil sistemlerin tamamen devre dışı kaldığı felaket senaryolarında dahi bankaların en geç yirmi dört saat içerisinde faaliyetlerini yeniden sürdürebiliyor olması gerekmektedir. Bu çerçevede yılda en az bir defa gerçek bir felaket senaryosunu sağlamaya yönelik testler yapılması beklenmektedir. Birincil veya ikincil merkez için dış hizmet halinde, veri merkezlerinin bulunduğu konumda veya bölgesel olarak yaşanacak gerçek bir felaket anında; birincil ve ikincil merkezdeki çalışma ortamının ve dış hizmet sağlayıcıların bankaya ayıracağı kaynağın, bankanın iş sürekliliğini sağlamayı garanti edecek nitelikte olması zorunluluğu getirilmiştir. Bilgi sistemleri süreklilik yönetimi sürecinin ulusal veya uluslararası bir standart ya da en iyi uygulamaları temel alması gerekliliği de açıkça belirtilmiştir.

Yönetmelik ile birlikte bankalardan, sunmakta oldukları bankacılık hizmetlerine yönelik reklam hizmeti aldıkları arama motoru, sosyal medya platformu gibi sağlayıcıların bankalar adına verilen sahte reklamları engellemeye yönelik tedbirleri alıp almadıklarını kontrol etmeleri beklenmektedir. Bankalardan, uygun tedbirleri almayan sağlayıcılardan reklam hizmeti alınmaması, bu hizmet sağlayıcılarla yapacağı sözleşmelerde, sahte reklam yayınlanması durumunda olaya özel her türlü bilgiyi alabileceğine dair hükümleri ekletmesi talep edilmektedir. Bankaların reklam hizmeti almak üzere anlaştığı aracı firmalar ile yapılan sözleşmeler de bu kapsama alınmıştır.

Yönetmelik'te kritik bilgi sistemleri ve güvenlik kapsamında alınacak ürün ve hizmetler için sağlayıcıların ve üreticilerin Türkiye'de müdahale ekiplerinin bulunması şartı ifade edilmiştir. Bu gerekliliğin, bu alanda ülkemize bir katma değer sağlayacağı aşikardır. Ayrıca bankalara, geçmişte bulut bilişim imkanlarından faydalanmalarına müsaade edilmezken, belirli şartlar altında dış hizmet olarak bulut bilişim hizmetlerini kullanabilme olanağı da sağlanmıştır.

Elektronik bankacılık alanındaki önemli noktalardan birisi de, bankaların elektronik ortamda müşterilerine ileteceği hassas veri veya sır niteliğinde veri içeren her türlü dekont, hesap özeti gibi bilgilerin elektronik bankacılık hizmeti sunulan kanallar üzerinden müşterilere gönderilebileceğidir. Ayrıca, bankalara elektronik bankacılık dağıtım kanallarından sunulmakta olan herhangi bir işlemin tersinin gerçekleştirilmesi mümkün ve orijinal işleme göre eşit ya da daha az riskliyse, orijinal işlemin tersi olan bu işlemlerin de aynı elektronik dağıtım kanalından gerçekleştirilmesini sağlama zorunluğu getirilmiştir.

BDDK, daha önce yayımlamış olduğu "Bankalarda Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ" ile ülkemizde önemli bir süreci başlatmış ve çeşitli sektörlerin bilgi sistemleri alanında düzenlenmesi konusunda öncü olmuştu. Yayımlanan bu Yönetmelik ile bilgi sistemleri alanında belirli bir olgunluk seviyesine gelmesi sağlanan Türk bankacılığında yeni bir dönemin başladığını söyleyebiliriz. Önümüzdeki dönemde, bankalarımızın teknoloji altyapılarının daha etkin ve güçlü hale geldiğini görürken, bu Yönetmelik'in diğer sektörlerimizdeki bilgi sistemleri mevzuatının da gelişmesine öncü olacağını düşünmekteyiz. Hepimizi bilgi sistemlerinden kaynaklı risklere de odaklanılan farklı bir gelecek beklediğini öngörüyoruz.

Yönetmelik, günlük teknoloji operasyonunu gerçekleştirdiğimiz her alanda halihazırda yapılmakta olan aktiviteleri düzenlerken, sektörün tüm paydaşlarının ortak bir dil, yaklaşım ve platforma sahip olmasını sağlayacaktır.

İletişim:

Cüneyt Kırlar
Ortak, Risk Danışmanlığı Lideri
ckirlar@deloitte.com

Barış Bağcı
Ortak, Risk Danışmanlığı
bbagci@deloitte.com

Metin Aslantaş
Ortak, Risk Danışmanlığı
maslantas@deloitte.com

© 2020. Daha fazla bilgi için Deloitte Türkiye (Deloitte Touche Tohmatsu Limited üye şirketi) ile iletişime geçiniz.