



## ISO 27001 Belgesi ile bilgi güvenliğinde dayanıklılığınızı artırın, müşterilerinizin güvenini kazanın ve rekabette avantajlı konuma geçin

"Sağlam sistemlerimiz olmazsa işlerimizi kaybedebiliriz. Bu yüzden standartları kullanma yolunu seçtik. En iyi uygulamaları kullanmayı başardığımızı, bunları ısrarla talep eden özel ve kamu sektöründeki müşterilerimize göstermek istedik."

Bill Millar,  
Güvenlik Bölümü Başkanı,  
Altyapı ve Dış Kaynak Hizmetleri,  
Capgemini UK

### Capgemini'nin hedefleri

- Yüksek güvenlik düzeyi ile kaynaklarını, çalışanlarını ve müşterilerinin bilgilerini koruma
- Rekabet avantajı kazanma
- Bilgi gizliliğinin, bütünlüğünün ve mevcudiyetinin sağlanması

### Capgemini'nin kazanımları

- Capgemini UK ve müşterileri için yüksek düzeyde güvenlik
- Potansiyel ve mevcut müşteriler için en iyi uygulamaları kullandığımızın belgeli kanıtı
- Yönetimin ve çalışanların güvenlik konusunda daha fazla farkındalık kazanmaları ve süreçleri desteklemeleri
- Gelişmiş düzeyde güvenlik dokümantasyonu ve raporlaması

### Capgemini Hakkında

Capgemini, Avrupa'nın en büyük Bilgi Teknolojileri hizmetleri sağlayıcısı olmasının yanı sıra, danışmanlık, teknoloji ve dış kaynak hizmet sağlama konularında da global bir liderdir.

Genel merkezi Paris'te bulunan şirketin bağımsız bir şirket olarak 45 yıllık bir geçmişi vardır ve şu anda 40'tan fazla ülkede ve 100'den fazla dilde hizmet vermektedir. 2012'de yıllık gelirinin 10,3 Milyar Euro olduğu bildirilmiştir.

### Neden belgelendirmeye ihtiyaç duydular?

Güvenlik, Capgemini grubunun dayandığı önemli bir yapı taşıdır; kaynaklarını, çalışanlarını ve varlıklarını (müşterilerinininkiler de dâhil olmak üzere) korur ve en nihayetinde şirkete rekabet avantajı sağlar.

Capgemini'nin temel güvenlik kapsamlarını kazalar, doğal afetler ve siber korsanların yaptığı saldırılar gibi geleneksel tehditlerin yanında, yasal gereklilikler, zorunlu yönetmelikler ve banka kartları sektörünün daha zorlu gereksinimleri gibi yeni "tehditler" oluşturur.

Capgemini'nin İngiltere'deki altyapı dış kaynak kullanımı hizmetlerinde Güvenlik Bölümü Başkanı olan Bill Millar yaklaşımlarını şöyle açıklıyor:

"Düzenlemelere uyum sağlayamazsak ağır cezalar alabilir ve itibarımıza ciddi zararlar verebiliriz. Güvenlik müşteriler için de önemli bir konu durumuna gelmiştir. Sağlam sistemlerimiz olmasa işlerimizi kaybedebiliriz. Bu yüzden standartları kullanma yolunu seçtik. En iyi uygulamaları kullanmayı başardığımızı, bunları ısrarla talep eden özel ve kamu sektöründeki müşterilerimize göstermek istedik."

Millar, işleri etkin bir şekilde yürütmek adına, bilgi gizliliğini, bütünlüğünü ve mevcudiyetini sağlamak için Capgemini UK'nin gerek duyduğu önlemleri belirledi. Bu önlemlerin pragmatik, iş odaklı, riske dayalı, bütüncül, sistematik, düşük maliyetli ve müşterinin ya da Capgemini'nin kendi standartları ile yönetilebilecek şekilde olması konusunda kararlıydı. Şirket bu doğrultuda, bilgi güvenliği konusunda kapsamlı bir yaklaşım sunan ISO/IEC 27001 Bilgi Güvenliği belgesi almayı amaçladı.

### Faydalar

ISO/IEC 27001 belgesi Capgemini UK'ye, kendileri ve müşterileri için gelişmiş güvenlik, yeni ve mevcut müşteriler için en iyi uygulama güvencesi, çalışanları için gelişmiş güvenlik farkındalığı gibi faydalar sağlamış olup, güvenlik dokümantasyonu ve raporlama konularında da ileri düzeyde bir sistem kurmalarına yardımcı olmuştur.

Güvenliğe artık üst yönetim düzeyinde oldukça değer veriliyor. Bu durum, operasyonel kabul ve mali destek oluşturarak güvenlik konusunu Capgemini UK'in Altyapı ve Dış Kaynak Hizmetleri departmanının bütüncül bir parçası yapıyor. En önemlisi de "Bu yalnızca verileri korumakla alakalı değil; insanları korumak ve fiziksel güvenlikle de alakalı, yani yalnızca teknik personele yönelik bir şey değil," diyor Millar.

Ve devam ediyor: "Belgelendirmenin bize sağladığı faydalardan çok memnunuz. Müşterilerimiz de bizi denetlemek adına dış kaynaklı denetçiler tutup, onlara ödeme yapmadıkları için memnunuz. Güvenliğimizin kalitesinden emin olmak için BSI'dan alınan raporlarımızı kullanıyorlar."

### Uygulama

ISO/IEC 27001 Bilgi Güvenliği Standardını şirketimizde ilk kullanan Capgemini'nin Hollanda ve Hindistan operasyonları oldu ve "Bundan açıkça fayda sağlıyorlardı," diyor Millar. Örneğin, Birleşik Krallık'taki şirketin ihalelere fiyat teklifi verirken her seferinde bir sürü doküman işi yaptığını ve bilgi güvenliği yetkinliğini kanıtlamak için oldukça fazla zaman ve para harcadıklarını söylüyor. "Yurtdışındaki meslektaşlarımız ise benzer durumlarda yalnızca ISO/IEC 27001 belge numaralarını sunuyorlardı. Sonra biz de, belgemizi alalım ve çalışanlarımızın başka işler yapabilmesine fırsat tanıyalım dedik."

Millar, gerekli yatırımı haklı çıkarmak için bir iş analizi oluşturdu ve kısa süre içerisinde hem mali açıdan hem de "destek" açısından yönetim kurulunun onayını aldı. "Zor olmadı. İşin aslı, yönetim kurulu 'Bunu şimdiye kadar neden yapmamışız?' diye sordu," diyor.

Miller, bu projenin kontrol yapısı olarak, Finans Direktörünün de desteğiyle Capgemini UK'in kendi Güvenlik Forumu'nu kullandı ve yalnızca bu işle ilgilenen iki kişilik bir ekip oluşturdu.

Öncelikle şirketin risk yaklaşımı netleştirildi ve daha sonra çalışanlarla iletişim kurularak müşteri sorumlularının desteği alınmaya başlandı. Ardından mobil güvenlik gibi yeni alanlar eklenerek güvenlik belgeleri güncellendi. Son olarak, başta kapsama alınan tüm alanlar sistematik olarak irdelenerek bir güvenlik denetimi döngüsü başlatıldı.

### BSI'nın rolü

Capgemini, denetleyici kuruluş olarak BSI'ı tercih etti. "BSI, projenin kapsamı konusunda tavsiyede bulunup kapsamımızı daraltmamızı ve görevi küçük lokmalar şeklinde tamamlamamızı (bu, işleri çok daha yönetilebilir duruma getirdi) önererek baştan beri çok yardımcı oldu" diyor Millar. "BSI'ı denetleyici kuruluş olarak seçtiğimizde sürecin aslında çok basit olduğunu ancak epey bir iş gerektirdiğini gördük."

Şöyle devam ediyor: "BSI'nın gerçekleştirdiği denetimler gerekli işleri yaptığımız için sorunsuz geçti. Denetim gayet düzgün bir şekilde gerçekleşti. Bizim ana görevimiz, üst yönetimden teknisyenlere kadar doğru kişilerin denetçileri görmek üzere hazır olmasını sağlamaktı."

Projenin başlangıcından yalnızca 10 ay sonra, Capgemini UK'in Dış Kaynak Hizmetleri sunan departmanı, bilgi güvenliği yönetimi sistemi için ISO/IEC 27001 belgesi alma amacına ulaştı. Şirket o zamandan beri BSI tarafından 6 ayda bir yapılacak şekilde takip denetimleri planladı.

Önümüzdeki dönemde diğer yeniden belgelendirmeler üç yılda bir yapılacak. Yeni hedefler, kalan son dört Birleşik Krallık tesisini belgelendirmenin yanı sıra Polonya ve Almanya dâhil olmak üzere grubun Birleşik Krallık dışındaki diğer operasyonlarına ISO/IEC 27001'in faydalarını anlatmayı içeriyor.



Bu dokümanda yer alan ticari markalar (örneğin BSI logosu veya "KITEMARK" sözcüğü) Birleşik Krallık genelindeki diğer bir çok ülkede İngiliz Standartları Enstitüsü'nün sahip olduğu tescil edilmiş ve tescil edilmemiş markalardır.