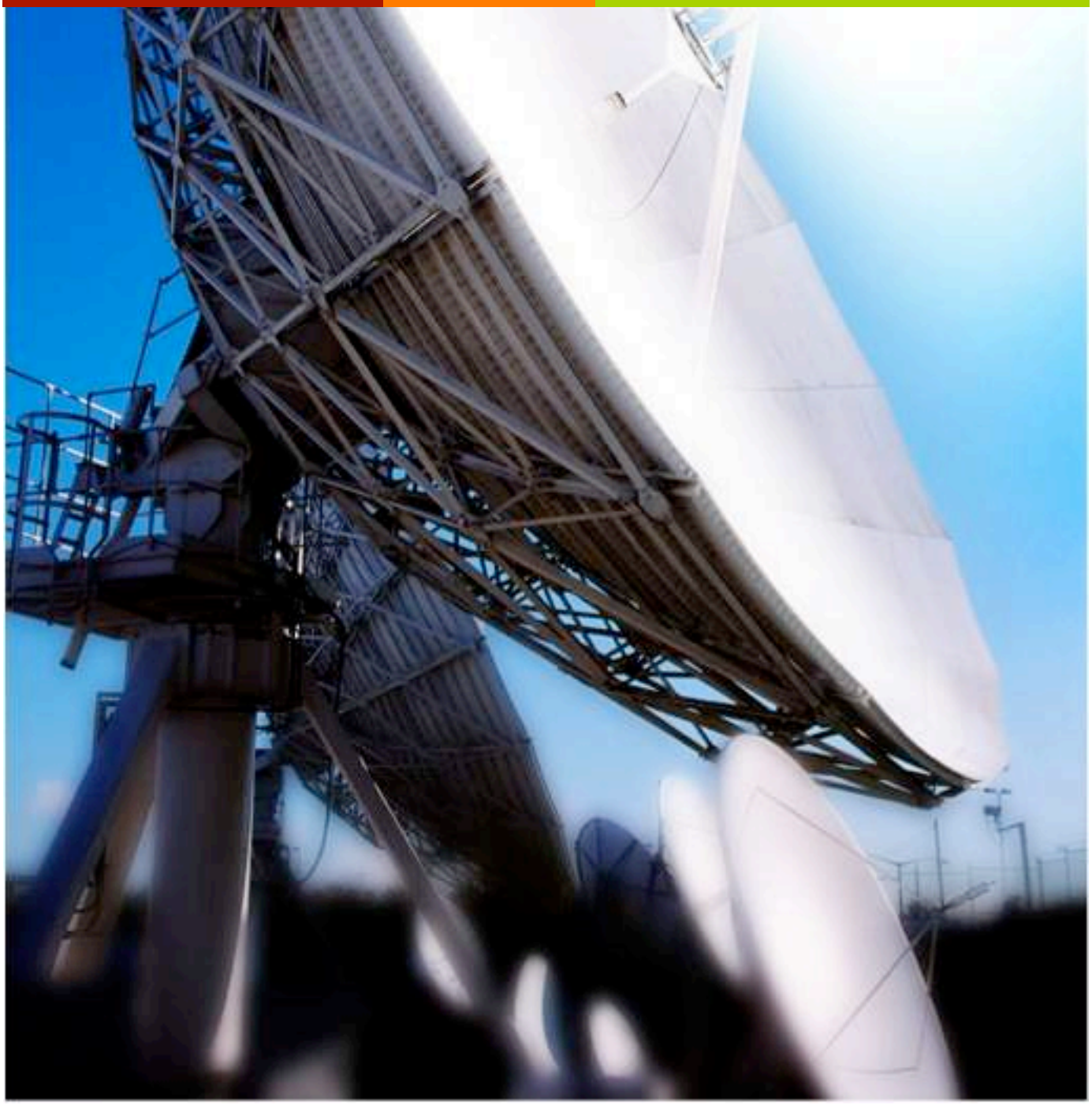
MerSis

Bilgi Teknolojileri
Bağımsız Denetim Hizmetleri



Bilgi Teknolojileri risklerinizin farkında mısınız ?

Bilgi Teknolojileri bağımsız denetim hizmetlerimiz, kuruluşların Bilgi Teknolojileri ile ilgili risk düzeylerini yansıtan raporların sunulması amacıyla geliştirilmiştir.

Bilginin zaman, mesafe ve hız kısıtlarından bağımsız hareket ettiği günümüz global bilgi toplumunda,

- Bilgiye ve Bilgi Teknolojilerine karşı artan bağımlılık,
- Bilgiye dayalı rekabetin yarattığı tehditler,
- Bilgi ve Bilgi Teknolojilerine yapılan yatırımların boyutları,
- Yeni iş fırsatları yaratma, maliyetlerin düşürülmesi vb. alanlarda teknolojinin sunduğu potansiyel ve dramatik değişiklikler nedeniyle,

bilgi ve Bilgi Teknolojilerinin (BT) etkin yönetimi, kuruluşların yaşaması ve başarısı için kritik önem arz etmektedir.

Birçok kuruluş, teknolojinin sağlıyabileceği potansiyel faydaları farkındadır. Ancak, yalnız yeni teknolojilerin yaratabileceği potansiyel riskleri farkında olup, bunları yönetenler başarılı olabilirler. BT ve ilişkili risklerin yönetimi, kurumsal yönetimin ağırlıklı konuları arasına girmiştir.

Bilgi ve destekleyen teknolojiler, birçok organizasyonun en önemli varlıkları konumuna gelmiştir. Yöneticilerin, doğru karar verebilmeleri için, güncel ve güvenilir bilgiye ihtiyacı vardır. Kritik iş süreçlerinin verimliliği Bilgi Teknolojilerinin kesintisiz çalışabilmesine bağlıdır.

Kuruluş üst düzey yönetimleri, Bilgi Teknolojileri ile ilgili riskleri yönetmek, ilgili hedefleri doğru belirlemek ve yönlendirebilmek amacıyla, bağımsız uzman görüşe ihtiyaç duymaktadır. Regülasyonlara tabi sektörlerde, bağımsız Bilgi Teknolojileri denetimleri zorunlu tutulmaktadır. Sermaye Piyasası Kurulları, şeffaflık ve güvenilirliği sağlamak amacıyla, finansal denetim raporları ile birlikte, Bilgi Teknolojileri denetim raporlarının da yayınlanmasını öngörmektedir.

Bilgi Teknolojileri bağımsız denetim hizmetlerimiz, yönetimlerin ihtiyaç duyduğu ve/veya yasal düzenlemeler gereği zorunlu tutulan, kuruluşların Bilgi Teknolojileri ile ilgili risk düzeylerini yansıtan raporların sunulması amacıyla geliştirilmiştir.

Information Technologies Governance Institute (ITGI) tarafından geliştirilmiş, Control Objectives for Information and Related Technologies (COBIT) Bilgi Teknolojileri Yönetim Modeli esas alınarak tasarlanan Bilgi Teknolojileri denetim hizmetlerimiz kapsamında, Planlama ve Organizasyon, Tedarik ve Uygulama, Hizmet Sunumu ve Destek ile İzleme ve Değerlendirme ana başlıkları altındaki süreçlere ilişkin genel kontrollar ile, uygulama kontrollarınız önemlilik ilkesi çerçevesinde denetlenmekte; Bilgi Teknolojileri yönetim süreçlerinizin olgunluk düzeyleri belirlenerek raporlanmaktadır.

Uygulama Kontrolları Denetimi

Uygulama kontrolları denetimi, Bilgi Teknolojileri içerisinde yer alan ve faaliyetlerinizi yürütmek veya desteklemek için kullanılan verilerin tanımlanması, üretilmesi, kullanılması, bütünlük ve güvenilirliğinin sağlanması, verilere erişimin yetkilendirilmesi gibi iç kontrolların etkinliğinin ve yeterliliğinin denetlenmesini ve değerlendirilmesini kapsamaktadır.

- Veri hazırlama prosedürleri
- Belge onay prosedürleri
- Belge toplama prosedürleri
- Hatalı belge düzeltme prosedürleri
- Belge saklama kontrolları
- Veri giriş onay prosedürleri
- Doğruluk ve bütünlük kontrolları
- Hatalı veri girişi düzeltme prosedürleri
- Veri işleme tutarlılık kontrolları
- Veri işleme doğrulama ve onaylama kontrolları
- Veri işleme hataları düzeltme prosedürleri
- Rapor üretimi ve saklama kontrolları
- Rapor dağıtım prosedürleri
- Rapor mutabakatları
- Rapor doğrulama ve hata düzeltme prosedürleri
- Hassas bilgi içeren raporların güvenliği

Bilgi Teknolojileri Bağımsız Denetimi Alanları

Genel Kontrol Alanları Denetimi

Genel kontrol alanları denetimi, COBIT Bilgi Teknolojileri Yönetim Modeli çerçevesinde, aşağıdaki süreç alanları kapsamında gerçekleştirilmektedir.

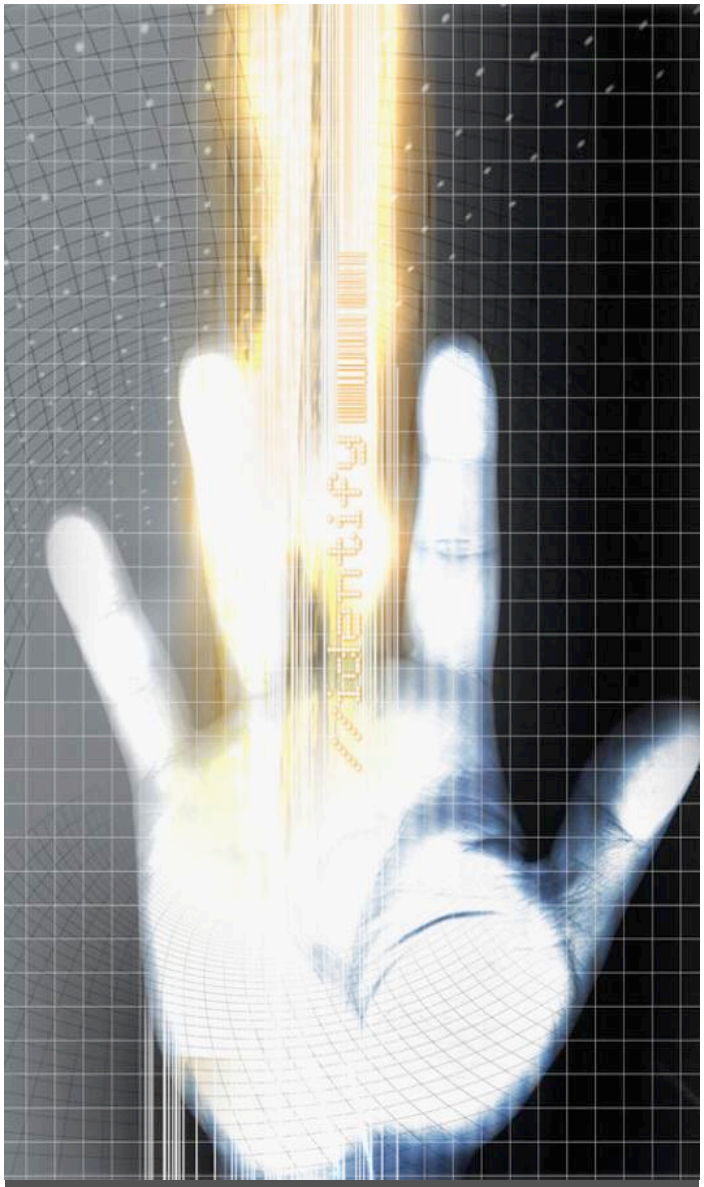
- **Planlama ve Organizasyon**
  - Stratejik Bilgi Teknolojileri planının tanımlanması
  - Bilgi mimarisinin tanımlanması
  - Teknolojik yönün belirlenmesi
  - Bilgi Teknolojileri süreçlerinin, organizasyonunun ve ilişkilerinin tanımlanması
  - Bilgi Teknolojileri yatırımlarının yönetimi
  - Yönetimin amaçlarının ve talimatlarının iletilmesi
  - İnsan kaynakları yönetimi
  - Kalite yönetimi
  - Bilgi Teknolojileri riskinin değerlendirilmesi ve yönetimi
  - Proje yönetimi

- **Tedarik ve Uygulama**
  - Otomasyon çözümlerinin belirlenmesi
  - Uygulama yazılımının geliştirilmesi ve bakımı
  - Teknoloji alt yapısının oluşturulması ve bakımı
  - Operasyon ve kullanımın sağlanması
  - Bilgi Teknolojileri kaynaklarının karşılanması
  - Değişiklik yönetimi
  - Sistem çözümlerinin ve değişikliklerin uygulanması ve akredite edilmesi

- **Hizmet Sunumu ve Destek**
  - Hizmet seviyelerinin tanımlanması ve yönetimi
  - Üçüncü kişilerden alınan hizmetlerin yönetimi
  - Performans ve kapasite yönetimi
  - Hizmet sürekliliğinin sağlanması
  - Sistem güvenliğinin sağlanması
  - Maliyetlerin belirlenmesi ve dağıtılması
  - Kullanıcıların eğitimi
  - Hizmet sunumu yönetimi ve olay yönetimi
  - Konfigürasyon yönetimi
  - Problem yönetimi
  - Veri yönetimi
  - Fiziksel çevre yönetimi
  - Operasyon yönetimi

- **İzleme ve Değerlendirme**
  - Bilgi Teknolojileri performansının izlenmesi ve değerlendirilmesi
  - İç kontrolün izlenmesi ve değerlendirilmesi
  - Denetlenenin iç usul ve esasları dahil ilgili mevzuata uyumun sağlanmas
  - Bilgi Teknolojilerine ilişkin kurumsal yönetişimin temini

Bilgi Teknolojileri bağımsız denetimlerimiz, öncesinde gerçekleştirilen risk değerlendirme çalışması sonucunda elde edilen veriler ışığında geliştirilen plan doğrultusunda, Information Systems Audit and Control Association (ISACA) tarafından tavsiye edilen 5 aşama takip edilerek gerçekleştirilmektedir.



Bilgi Teknolojileri Bağımsız Denetimi Sürecimiz

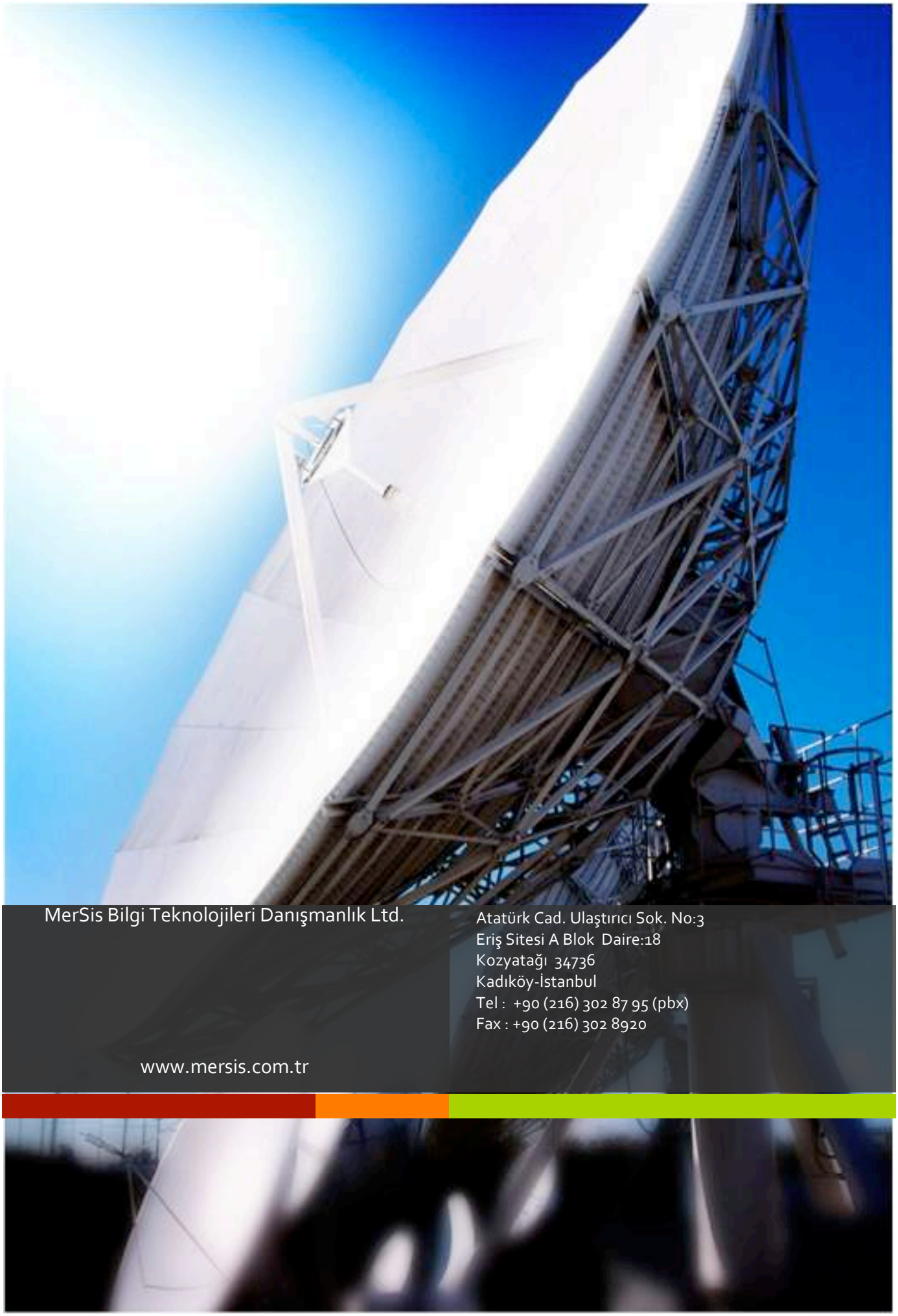
- **Tanımlama ve Dokümantasyon Aşaması**
  - Denetim Yönergesi ile belirlenen dokümanlar incelenir.
  - Denetim Yönergesi ile belirlenen kişiler ile görüşülür.
  - İnceleme ve görüşmeler neticesinde, denetlenen süreç ile ilgili faaliyetlerin kimler tarafından, nerelerde, ne zaman, hangi prosedürler doğrultusunda, hangi girdileri kullanarak ve hangi çıktıları üreterek gerçekleştirildiği belirlenir ve dokümante edilir.

- **Değerlendirme Aşaması**
  - İlk aşamada tanımlanan süreç ve kontrollerin, Denetim Yönergesi ile belirlenen beklentiler ile uyumu ve etkinliği değerlendirilir ve dokümante edilir.
  - Uyumsuzluktan kaynaklanan riskleri önleyebilecek, alternatif kontrollerin varlığı ve yeterliliği değerlendirilir ve dokümante edilir.
  - Tanımlı süreç ve kontrollerin yeterli görülmesi durumunda "Denetim" aşaması, aksi durumda "Risk Belirleme" aşaması gerçekleştirilir.

- **Denetim Aşaması**
  - Denetim Yönergesi ile belirlenen iş ürünleri örnekleme yöntemi ile seçilerek, tanımlı süreç ve kontroller ile uyumları test edilir.
  - Faaliyetlerin tanımlı süreç ve kontroller ile uyumsuz sürdürüldüğü saptandığı taktirde, mevcut uygulanan süreç ve kontrollerin tanımlanması gerçekleştirilir.

- **Risk Belirleme Aşaması**
  - Denetim Yönergesi ile belirlenen değerlendirmeleri yapmak üzere gerekli iş ürünleri, Örnekleme Yönergesi doğrultusunda, istatistiksel örnekleme yöntemleri kullanılarak seçilir.
  - Seçilen örnek kümesi kapsamında, Denetim Yönergesi ile belirlenen kriterlerin karşılanıp karşılanmadığı değerlendirilir.

- **Raporlama Aşaması**
  - Süreç ile ilgili elde edilen veriler, değerlendirmeler ve sonuçlar Süreç Denetim Raporu formatında dokümante edilir.



MerSis Bilgi Teknolojileri Danışmanlık Ltd.

Atatürk Cad. Ulaştırıcı Sok. No:3
Eriş Sitesi A Blok Daire:18
Kozyatağı 34736
Kadıköy-İstanbul
Tel : +90 (216) 302 87 95 (pbx)
Fax : +90 (216) 302 8920

www.mersis.com.tr