İÇ KONTROL NEDİR?

Kurumlar gerek çalışanları gerek hissedarları için; operasyonel döngü içerisinde maksimum karlılık ve uzun süreli devamlılık amacıyla kurulur ve çalışırlar.

Ancak söz konusu amaçlarına ulaşmalarının önünde birçok engel bulunabilir.

Bu engellere aynı zamanda “Risk” de diyebiliriz.

Riskler organizasyon içinden gelebileceği gibi dış faktörlerin de bir sonucu olabilir

Yönetim zafiyetleri, kontrolsüz iş akışları, kişiye bağımlı süreçler, çevre, küresel iktisadi ve sosyolojik dalgalanmalar, yasalar ile uyumsuzluk risklere örnek olarak sayılabilir.

Bütün bu risklere kendileri ile beraber suistimal riskini de beraberinde getirmektedir.

Bu bilgiler ışığında, uluslararası düzeyde kabul gören COSO çerçeve tanıma göre, **iç kontrol**; kurumların hedeflerine ulaşmasının önündeki engelleri kaldırmak (*riskleri bertaraf etmek*) ve hedeflere ulaşıldığına dair makul güvence sağlamak üzere **tasarlanmış** sistemler bütünüdür.

Tasarlanmış Sistemin Aktörleri

COSO standartlarında kurumlar içinde iç kontrol sistemini tasarlayacak ve uygulayacak “3’lü Savunma Hattı” aktörleri şöyle tanımlanır;

- Yönetim tarafından üstlenilen iç kontrolleri işleten icracı birimler
- Bağımsız çalışan İç Kontrol birimi
- Bağımsız çalışan İç Denetim birimi

Bu aktörlere ek olarakYönetim Kuruluna bağlı ve deneyimli Denetim Komitesi’nin varlığı da çok önemli bir unsurdur.

İç Kontrol Sisteminin Amaçları

- İşletme varlıklarını korumak, her anlamda kayıpları önlemek
- Muhasebe verilerinin doğru ve güvenilir olmasını sağlamak
- İşletme faaliyetlerinin etkinliğini arttırmak
- Yönetim politika ve prosedürlerine bağlılığı arttırmak

*6102 Sayılı TTK; **iç kontrol**, **iç denetim** ve **risk yönetimi** konusunda sadece **Yönetim Kurulunun** karar alabileceği, esas sözleşme ile dahi olsa, bu konu ile ilgili kararların genel kurul dâhil başka herhangi bir organa bırakılamayacağı açıkça ifade edilmiştir.*

İÇ DENETİM

Uluslararası İç Denetçiler Enstitüsü tarafından yapılan tanımıyla İç Denetim; Bir kurumun operasyonlarını geliştirmek ve onlara değer katmak için tasarlanmış “**bağımsız**” ve “**nesnel**” güvence ve danışmanlık faaliyetidir.

Risk yönetimi, kontrol ve yönetişim süreçlerinin verimliliğini değerlendirme alanında disiplinli ve sistematik bir yaklaşım getirerek kurumun hedef ve amaçlarına ulaşmasına yardımcı olur.

İç denetimin en önemli görevi, kurumun iç kontrol mekanizmalarının etkinliğine ilişkin makul bir güvence vermektir.

Denetim fonksiyonu organizasyon içi bağımsız denetim birimleri tarafından sağlanabileceği gibi yetkin dış kaynaklar tarafından da sağlanabilir.

COSO; İÇ KONTROL STANDARTLARI

COSO (Committee of Sponsoring Organizations of the Treadway Commission) 1985 yılında, iç kontrol, risk yönetimi, kurumsal yönetim ve suiistimali önleme alanlarında kapsamlı bir uygulama rehberi hazırlamak adına, kurulmuş organizasyondur.

Organizasyonun koyduğu standartlar günümüzde dünya genelinde en fazla kabul gören ve uygulanan iç kontrol çerçevesidir.

Ana hedefi; iç kontrolün tanımını yapmak ve sağlıklı bir iç kontrol ortamı yaratmak için gerekli unsurları ortaya koymaktır. Bu unsurlar aşağıda iki grup halinde verilmiştir:

I. COSO iç kontrol ana başlıkları;

- Finansal Raporlama Güvenilirliği
- Yasa ve Kanunlar ile Uyum,
- Operasyonlarda Etkinlik ve Verimlilik

Görüleceği üzere “ana başlıklar” iç kontrol sisteminin amaçları ile örtüşmektedir.

II. COSO iç kontrol bileşenleri;

- Kontrol Ortamı Yaratılması
- Risk Değerlemesi Yapılması
- Kontrol Aktivitelerinin Kurgulanması
- Bilgi ve İletişimin Etkin Kullanılması
- Gözetim ve İzleme Yapılması

İç kontrol “bileşenleri” sistemin etkin çalışmasını destekleyecek işleyiş adımlarıdır.

CobIT NEDİR?

CobIT “Bilgi ve İlgili Teknolojiler İçin Kontrol Hedefleri” anlamına gelmektedir.

Uluslararası mesleki enstitüler olan ISACA ve ITGI tarafından geliştirilmiş, Bilgi Teknolojileri (BT) yönetimi için kabul edilen en iyi uygulamalar kümesidir.

CobIT başlı başına bir süreç olmayıp, güçlü bir yönetim ve kontrol önerileri bütünüdür.

Temelde CobIT, BT kaynakları olan insan, yazılım, donanım ve bilgiyi en etkin süreçler ile işleyerek, kurumun ihtiyaç duyduğu iş gereksinimlerini karşılamaya çalışır.

CobIT, genel anlamda dört ana başlık altında yönetim önerileri getirir ve kontrol noktaları belirler:

- Planlama ve Organizasyon
- Tedarik ve Uygulama
- Teslimat ve Destek
- İzleme ve Değerlendirme

DENETİM HİZMETLERİMİZ

COSO ve CobIT standartları çerçevesinde verdiğimiz iç denetim hizmetlerinde işletmelerde riski azaltmaya, dinamik ve katma değerli, proaktif stratejiler oluşturmaya çalışmaktayız.

A. Risk Odaklı İç Denetim Hizmetleri

Risk odaklı iç denetim hizmetimiz temelde; İşinizi ve operasyonlarınızı anlamak, süreçlerinizin ve kontrollerinizin etkinliğini test etmek, kontrol eksikliklerini belirlemek ve daha sonra ihtiyaçlarınıza uygun, uygulanabilir iç denetim çözümleri önermek adımlarını içerir.

Öne çıkan iç denetim hizmetlerimiz;

- Dış kaynaklı iç denetim hizmetleri
- İç kontrol incelemeleri ve süreç haritalama
- Risk yönetimi incelemesi
- Kurumsal yönetişim incelemesi
- Düzenleyici kurumların gerektirdiği şekilde uyumluluk denetimleri
- SOX denetimleri

B. Risk Danışmanlığı

a. İşletme Risk Danışmanlığı

İşletme Risk Danışmanlığı ile sizlere Risk Yönetişimi ve Risk Yönetimi çerçevesinde yardımcı olmaktayız.

Risk Yönetişimi; yönetim politikaları ve uygulamaları olarak tanımlanabilir.

- Risk yönetimi stratejisinin oluşturulması,
- Risk yönetimi yapısı, bileşimi ve işlevleri oluşturmak,
- Risk Yönetimi Komitesi ve tüzüklerini oluşturmak,
- Risk Yönetimi Başkanı ve risk yönetimi ekibinin görev ve sorumluluklarını tanımlamak,
- Risk yönetimi politikaları ve prosedürleri el kitaplarının geliştirilmesi.
- SOX gereklilik uyarlamaları

Risk Yönetimi; belirlenmiş risk önleyici faaliyetlerin fiilen sahada uygulanmasıdır. Bir risk yönetimi çerçevesi geliştirmenize aşağıdaki yollarla yardımcı olabiliriz:

- Risk ortamınızı belirlemek,
- Risk oluşma olasılığı ve bunların işletmeniz üzerindeki etkilerinin tespiti
- Riskleri işiniz açısından önem açısından önceliklendirme,
- Risk izleme ve raporlama mekanizmasının geliştirilmesi.

b. İç Kontrol İncelemesi

İç Kontrol İncelemesi, mevcut ekonomik ve hızla gelişen sistemler bütününde daha büyük önem taşımaktadır.

Uygulanan iç kontrol sisteminin Yönetim Kurulu'nun öngördüğü, yayınladığı kurallar çerçevesinde etkili olup olmadığından emin olmak için iç kontrollerin “çeşitli fonksiyonlar arasında” izlenmesi ve değerlendirilmesi amacıyla uygulanır.

Özetle; iç kontrol sisteminin genel bir değerlendirmesi olup, işletmedeki her bir iş alanının riskleri ele alma yeterliliğini ve etkinliğini ortaya koymayı hedefler. İleri düzeyde düzeltici faaliyetler için iç kontrol eksikliklerinin tanımlanmasını kolaylaştırır.

c. Teknoloji Risk Danışmanlığı

Risklerinizi başarıyla yönetmek ve katma değerli ürün ve hizmetler oluşturmak için Bilgi Teknolojilerinden (BT) yararlanmak evrensel bir iş uzmanlığı haline gelmiştir.

Teknoloji Risk Danışmanlığı kapsamında aşağıdaki hizmetleri sunuyoruz:

CobIT 4.1 BT Yönetişim / Yönetim Çerçevesi
BT yönetişim hizmetleri kapsamında, aşağıdakileri geliştirmenize yardımcı olabiliriz:

- BT yönetimi ile şirket yönetim eşgüdümü
- Sistem geliştirme yaşam döngüsü
- İşletim sistemi, uygulamalar, veri tabanı kontrolleri
- Fiziksel güvelik: Sistem odası-veri merkezleri
- Veri yedekleme ve yedekten geri dönme
- Sistem operasyonları yönetimi (iş planlama)

BT Kimlik Yönetimi ve Yetkilendirme
Kuruluşunuza aşağıdaki yollarla yardımcı olabiliriz:

- Çalışanlar ve yetkiler analizi
- Görevler ayrılığı prensibinin uygulanması
- Periyodik testler ve uygulamalar

Uygulama, Veri Tabanı, İşletim Sistemi Güvenliği
Bilgi Sistemi katmanlarında alınacak güvenlik önlemleri veya bunların test edilmesi amacıyla:

- Güvenli bağlantı protokol yöntemleri,
- Güvenlik konfigürasyonları
- Loglama mekanizmaları
- Logların alarmlara bağlanması ve izlenmesi,
- Şifre politikaları,
- Kriptolama (encryption), veri maskeleme,
- Yönetici / anonim hesaplar yönetimi,

Veri Yedekleme Yönetimi
Kurumsal verinizin kaybolmaması ve operasyonlarınızın kesintiye uğramaması için size şu işlemlerde yardımcı olabiliriz:

- Süreç yönetimi
- Yedekleme yöntemleri
- RPO – Kurtarma Noktası Hedefi
- RTO – Kurtarma Zaman Hedefi
- Aynı ve farklı konumlarda yedekleme
- Yedekten geri dönme testleri

Bilgi Güvenliği
Bilginin Gizliliği, Bütünlüğü, Erişilebilirliği konularında size şu işlemlerde yardımcı olabiliriz:

- Bilgi envanterinin çıkarılması
- Sınıflandırılması
- Sahiplendirilmesi
- Uygun iç kontrollerin tasarlanması