Denetci.org

REFERANS İLKELERİ

İç Kontrol İlkeleri

Rİ-YON-4

Sürüm 1.0 · 11.08.2026

www.denetci.org

İç Kontrol İlkeleri

İç kontrol, bir kuruluşun amaçlarına ulaşmasını, kaynaklarını korumasını, güvenilir bilgi üretmesini ve hata, suistimal veya yetkisiz davranışların etkisini sınırlandırmasını destekleyen tasarım anlayışıdır. Amaç mümkün olan en fazla kontrolü oluşturmak veya işlemleri onay ve kayıt katmanlarıyla çevrelemek değil; önemli belirsizlik ve risklerin işin doğal yapısı içinde anlamlı biçimde sınırlandırıldığı, sapmaların fark edilebildiği ve kontrolün gerçekten çalışıp çalışmadığının doğrulanabildiği bir yapı kurmaktır.

İlke 1: Her kontrol açık bir risk veya güvence ihtiyacına dayanmalıdır.

Bir kontrolün neden var olduğu ve hangi hata, suistimal, kayıp veya belirsizliği azaltması beklendiği açıklanabilmelidir. Geçmişten beri uygulanıyor olması veya yaygın bir uygulama olması tek başına devam etmesi için yeterli gerekçe değildir.

İlke 2: Kontrolün amacı kontrolün biçiminden daha önemli olmalıdır.

Onay, imza, rapor, mutabakat veya başka bir mekanizma yalnızca bir araçtır. Kontrol, hedeflediği risk üzerinde gerçek bir etki oluşturmuyorsa biçimsel olarak uygulanması güvence sağlamaz.

İlke 3: Kontrol sayısı güvence düzeyi olarak yorumlanmamalıdır.

Çok sayıda tekrar eden veya aynı varsayıma bağlı kontrol, daha güçlü bir yapı yerine daha fazla karmaşıklık oluşturabilir. Güvence, kontrol miktarından çok önemli risklere karşı sağlanan gerçek ve bağımsız etkiden doğmalıdır.

İlke 4: Kontroller mümkün olduğu ölçüde işin doğal çalışma biçiminin parçası olmalıdır.

İş sürecinden kopuk ve sonradan eklenmiş kontrol adımları zamanla biçimselleşebilir veya çevresinden dolaşılabilir. Doğru davranışın sürekli özel dikkat gerektirmeden ortaya çıkması, yalnızca hatayı sonradan yakalamaktan daha dayanıklı olabilir.

İlke 5: Kontrol tasarımı hem hata hem bilinçli kötüye kullanım ihtimalini dikkate almalıdır.

İnsanlar yanlış karar verebilir, önemli bir ayrıntıyı atlayabilir veya kendilerine verilen yetkiyi kötüye kullanabilir. Kontrol, yalnızca iyi niyetli ve dikkatli kullanıcıların beklenen yolu izleyeceği varsayımına dayanmamalıdır.

İlke 6: Bir hata veya suistimalin etkisi gereksiz biçimde tek bir karar ya da kişide yoğunlaşmamalıdır.

Tek bir tarafın kritik bir işlemi başlatabilmesi, onaylayabilmesi, gerçekleştirebilmesi ve sonuçlarını değiştirebilmesi hata veya kötüye kullanım etkisini büyütebilir. Kontrol ayrımı organizasyon unvanlarından çok gerçek karar ve işlem yetkilerine dayanmalıdır.

İlke 7: Görev ayrımı kendi başına amaç haline gelmemelidir.

Her faaliyetin birden fazla kişi tarafından yürütülmesi her zaman daha güçlü güvence oluşturmaz. Ayrım, gerçekten bağımsız muhakeme veya etki sınırı sağladığı ölçüde değer taşımalıdır.

İlke 8: Tam görev ayrımının mümkün olmadığı durumlarda kalan risk görünmez bırakılmamalıdır.

Küçük ekipler veya özel operasyonlar bazı yetkilerin aynı tarafta birleşmesini gerektirebilir. Bu durumda yapı güvenliymiş gibi varsayılmamalı; tek noktada toplanan etkinin nasıl sınırlandırılabileceği ayrıca düşünülmelidir.

İlke 9: Yetki gerçek sorumluluk ve işlem ihtiyacıyla sınırlı olmalıdır.

Bir tarafın işini yapabilmesi için gerekenin üzerindeki yetki, hata ve suistimalin olası etkisini artırır. Kolaylık veya geçmiş kullanım gereksiz geniş yetkinin kalıcı gerekçesi haline gelmemelidir.

İlke 10: Bir işleme yetkili olmak her kullanımın uygun olduğu anlamına gelmemelidir.

Bazı yetkiler yalnızca belirli koşullarda, amaçlarda veya işlem büyüklüklerinde anlamlı olabilir. Kontrol modeli gerektiğinde yetkinin varlığının yanında kullanım bağlamını da dikkate almalıdır.

İlke 11: Kontrol kararı gerçek bir değerlendirme içermelidir.

Bir işlemin başka bir kişi tarafından görülmesi veya onaylanması tek başına bağımsız kontrol oluşturmaz. Kontrolü gerçekleştiren tarafın neyi değerlendirmesi gerektiğini anlayabilmesi ve gerektiğinde işlemi sorgulayabilmesi gerekir.

İlke 12: Daha fazla onay katmanı otomatik olarak daha fazla güvence oluşturmamalıdır.

Aynı bilgiye dayanan ve birbirinin kararını sorgulamayan çok sayıda onay, tek bir anlamlı değerlendirmeden daha güçlü olmayabilir. Kontrol gücü rol sayısından değil bağımsız ve yeterli muhakemeden doğmalıdır.

İlke 13: Kontrol eşikleri gerçek etkinin yapay biçimde parçalanmasıyla aşılmamalıdır.

Bir işlemin daha küçük parçalara bölünmesi veya farklı teknik yollarla gerçekleştirilmesi aynı toplam sonucu üretebilir. Kontrol, yalnızca tekil işlem biçimine değil ortaya çıkan gerçek etkiye göre anlamını korumalıdır.

İlke 14: Kontrol müdahale edebileceği kadar erken noktada anlam taşımalıdır.

Bir hata ancak geri döndürülmesi çok zor hale geldikten sonra fark ediliyorsa kontrolün önleyici değeri sınırlıdır. Kontrol noktası, hedeflediği riski gerçekten etkileyebileceği bir konumda bulunmalıdır.

İlke 15: Kontrol yalnızca kontrol edilen tarafın ürettiği bilgiye bütünüyle bağımlı olmamalıdır.

Bir kontrolün bütün girdileri aynı hata veya manipülasyon kaynağından geliyorsa görünürde bağımsız bir değerlendirme gerçekte aynı varsayımı tekrar ediyor olabilir. Kritik güvence gerektiğinde farklı veya daha güvenilir kanıt kaynaklarına dayanabilmelidir.

İlke 16: Manuel kontrol insanın gerçek değerlendirme kapasitesini aşmamalıdır.

Aşırı hacim, tekrar veya karmaşıklık altında insan kontrolü kolayca biçimsel bir işarete dönüşebilir. İnsan muhakemesine dayanan kontrol, insanın gerçekten ayırt edebileceği ve değerlendirebileceği bir çalışma biçimine sahip olmalıdır.

İlke 17: Otomatik kontrol kusursuz ve değişmez kabul edilmemelidir.

Otomasyon tutarlılığı artırabilir; ancak yanlış mantığı büyük ölçekte uygulayabilir veya değişiklik sonrasında beklenmeyen sonuç üretebilir. Otomatik kontrolün güveni, gerçek davranışının ve onu belirleyen kuralların güvenilirliğine dayanmalıdır.

İlke 18: Kontrolün başarısızlığı sessiz normal durum gibi görünmemelidir.

Bir kontrol çalışmadığında, veri alamadığında veya beklenen değerlendirmeyi gerçekleştiremediğinde süreç kontrol edilmiş gibi devam etmemelidir. Kontrol kapasitesinin kaybı, sağladığı güvenin de azaldığı anlamına gelmelidir.

İlke 19: Telafi edici kontrol yalnızca başka bir kontrolün varlığı anlamına gelmemelidir.

Beklenen mekanizma uygulanamıyorsa alternatif yaklaşım aynı riski gerçekten anlamlı ölçüde azaltmalıdır. Farklı isimde veya farklı yerde başka bir kontrol bulunması eşdeğer güvence sağladığını göstermez.

İlke 20: İstisna kontrol sisteminin dışında bir alan oluşturmamalıdır.

Kontrolün uygulanamadığı veya bilinçli olarak aşılmasının gerekli olduğu durumlar olabilir. İstisna, kontrol ihtiyacının ortadan kalktığı varsayımı değil; farklı koşullar altında verilmiş sınırlandırılmış bir risk kararı olarak ele alınmalıdır.

İlke 21: Geçici kontrol sapmaları kalıcı çalışma biçimine dönüşmemelidir.

Acil durum, iş sürekliliği veya başka geçici ihtiyaçlar normal kontrolden farklı davranmayı gerektirebilir. Bu yollar ihtiyaç sona erdikten sonra görünmez biçimde günlük işleyişin kolay alternatifine dönüşmemelidir.

İlke 22: Kontrol, kendi çevresinden dolaşılabilen gerçek işlem yollarını dikkate almalıdır.

Bir süreçte güçlü kontrol bulunurken aynı sonuca doğrudan sistem erişimi, alternatif kanal veya başka yöntemle ulaşılabiliyorsa gerçek kontrol gücü daha zayıf olan bu yolla belirlenir. Değerlendirme yalnızca resmî süreç akışına bağlı kalmamalıdır.

İlke 23: Kontrol kanıtı kontrolün gerçekte ne yaptığını gösterebilmelidir.

Bir kaydın, işaretin veya onayın bulunması kontrolün gerçek değerlendirmeyi gerçekleştirdiğini her zaman göstermez. Kanıt, mümkün olduğu ölçüde kontrolün ilgili işlem veya risk üzerinde beklenen davranışı ürettiğini desteklemelidir.

İlke 24: Kontrolün etkinliği tamamlanma oranından veya hata bulunmamasından çıkarılmamalıdır.

Kontrollerin yüzde yüz uygulanmış görünmesi doğru şeyi kontrol ettiklerini göstermez; hiçbir sapma bulunmaması da kontrolün güçlü olduğunu kanıtlamaz. Etkinlik, hedeflenen riskin gerçek davranışta ne ölçüde sınırlandırıldığı üzerinden değerlendirilmelidir.

İlke 25: Tekrarlanan kontrol sorunları tekil insan hataları olarak görülmemelidir.

Aynı sapma sürekli ortaya çıkıyorsa kontrol tasarımı, süreç, teşvikler, yetki modeli veya başka sistemik nedenler yetersiz olabilir. Kontrol sistemi tekrar eden belirtilerden daha temel nedenleri öğrenebilmelidir.

İlke 26: Kontrol maliyeti ve oluşturduğu yeni davranışlar güvence tasarımının parçasıdır.

Aşırı yavaş, karmaşık veya maliyetli kontroller insanların işlerini alternatif yollarla yürütmesine neden olabilir. Kontrolün değeri yalnızca risk azaltımı değil, oluşturduğu ek karmaşıklık ve yeni hata alanlarıyla birlikte değerlendirilmelidir.

İlke 27: Kontrol sonuçları karar verebilecek taraflara anlamlı biçimde ulaşabilmelidir.

Bir sapmanın raporda bulunması, gerekli tarafların onu anlayıp uygun karar verebildiği anlamına gelmez. Kontrol bilgisi ilgili riskin gerçek önemini gösterecek bağlamda kullanılabilir olmalıdır.

İlke 28: Kontrolü geçersiz kılma gücü kontrol modelinin görünmez dışında kalmamalıdır.

Yönetim veya yüksek yetkili tarafların bazı kontrolleri aşabilmesi gerekli olabilir. Ancak bu güç sınırsız ve izsiz olduğunda diğer kontrollerin gerçek güvencesini önemli ölçüde azaltabilir.

İlke 29: İç kontrol sistemi değişen iş ve risk koşullarıyla birlikte yeniden anlamlandırılmalıdır.

Süreç, teknoloji, insan, dış bağımlılık veya amaç değiştiğinde geçmişte uygun olan kontrol aynı riski artık azaltmıyor olabilir. Kontrollerin varlığı değil, güncel güvence ihtiyacıyla ilişkisi korunmalıdır.

İlke 30: İç kontrol güvencesi gerçek işlem ve sonuç davranışı üzerinden doğrulanabilmelidir.

Kontrol matrisleri, prosedürler, onay kayıtları veya uygulama ekranları tek başına güvence oluşturmaz. Önemli risklerin gerçek işlemlerde nasıl sınırlandırıldığı, kontrollerin çevresinden

hangi yollarla dolaşılabildiği ve sapma ortaya çıktığında sistemin gerçekten nasıl davrandığı gerektiğinde gösterilebilmelidir.