Denetci.org

REFERANS İLKELERİ

İç Denetim İlkeleri

Rİ-GUV-2

Sürüm 1.0 · 11.08.2026

www.denetci.org

İç Denetim İlkeleri

İç denetim, kuruluşun yönetişim, risk yönetimi, iç kontrol ve diğer güvence düzeneklerinin gerçekte nasıl çalıştığına ilişkin bağımsız değerlendirme sağlar. Amaç mümkün olan en fazla bulguyu üretmek, kontrol listelerini tamamlamak veya yönetimin mevcut anlatısını doğrulamak değil; önemli güvence iddialarını yeterli ve güvenilir kanıtla sınamak, belirsizliği dürüstçe göstermek ve karar vericilere kuruluşun gerçek durumuna ilişkin kullanılabilir güvence sunmaktır.

İlke 1: İç denetim bağımsız muhakemeyi korumalıdır.

Denetim sonucu denetlenen tarafın, yönetimin veya başka bir çıkar sahibinin tercih ettiği sonuca göre şekillenmemelidir. Bağımsızlık yalnızca organizasyon şemasındaki konum değil, gerektiğinde rahatsız edici sonuçları kanıta dayanarak ifade edebilme kapasitesidir.

İlke 2: Tarafsızlık görüş sahibi olmamak değil kanıtın görüşten üstün olmasıdır.

Denetçi deneyim ve muhakeme kullanır; ancak kişisel yakınlık, çatışma, çıkar veya ön kabul sonucu belirlememelidir. Benzer kanıtlar benzer koşullarda makul ölçüde tutarlı değerlendirmelere yol açabilmelidir.

İlke 3: Denetçi denetlenen faaliyetin gerçek sahibi haline gelmemelidir.

Denetçi görüş verebilir ve iyileştirme seçeneklerini tartışabilir; ancak yönetimin kararını, kontrolünü veya operasyonel sorumluluğunu devraldığında daha sonra aynı alan hakkında bağımsız güvence verme kapasitesi zayıflar.

İlke 4: Denetim kapsamı gerçek risk ve güvence ihtiyacından türemelidir.

Kolay denetlenebilen, geçmişten alışılmış veya yüksek görünürlüğe sahip alanlar daha önemli risklerin önüne otomatik olarak geçmemelidir. Denetim önceliği kuruluşun amaç, değişiklik, bağımlılık ve maruziyetlerini yansıtmalıdır.

İlke 5: Denetim planı değişmeyen takvim olmamalıdır.

Yeni olaylar, önemli değişiklikler veya yeni risk bilgileri önceki öncelikleri değiştirebilir. Geçmişte verilmiş yıllık kararlar kuruluşun değişen gerçekliğinin önüne geçmemelidir.

İlke 6: Denetim evreni organizasyon şemasından daha geniş olmalıdır.

Ürünler, hizmetler, projeler, veri akışları, platformlar, dış bağımlılıklar ve kuruluş genelindeki ortak güven yapıları birden fazla organizasyon birimini kesebilir. Riskin gerçek sınırı idari bölüm sınırlarıyla aynı olmak zorunda değildir.

İlke 7: Her denetim açık bir güvence sorusuna dayanmalıdır.

“Bu alan denetlendi” ifadesi kendi başına hangi sonucun değerlendirildiğini göstermez. Denetim, hangi iddia, risk veya sistem davranışı hakkında güvence üretmek istediğini açıklayabilmelidir.

İlke 8: Kullanılan denetim yöntemi cevaplanmak istenen soruya uygun olmalıdır.

Doküman incelemesi tasarım niyetini gösterebilir ancak gerçek uygulamayı kanıtlamayabilir; örnekleme bazı davranışları gösterir ancak bütün kitle hakkında mutlak kesinlik sağlamaz. Yöntem alışkanlığa değil gerekli kanıtın niteliğine göre seçilmelidir.

İlke 9: Denetimin kapsam ve kesinlik sınırları görünür olmalıdır.

Belirli sistemler, dönemler veya işlem türleri incelenmemiş olabilir. Sonuç, kullanılan kanıtın desteklemediği alanlara veya kesinlik düzeylerine genişletilmemelidir.

İlke 10: Kapsam dışında kalan alanlar hakkında örtük güvence üretilmemelidir.

Bir raporun okuyucusu incelenmemiş alanların da değerlendirilmiş olduğunu varsaymamalıdır. Nelerin sınanmadığı, sonucu doğru yorumlamak için önemliyse açık kalmalıdır.

İlke 11: Denetim mevcut anlatıyı doğrulamak için değil gerçekliği sınamak için yürütülmelidir.

Yönetim beyanları, süreç açıklamaları ve geçmiş değerlendirmeler yararlı başlangıç bilgileri olabilir; ancak kendi doğruluklarının kanıtı değildir. Önemli varsayımlar gerektiğinde sorgulanabilmelidir.

İlke 12: Mesleki şüphecilik otomatik güvensizlik veya karşıtlık anlamına gelmemelidir.

Denetçinin görevi her açıklamayı yanlış kabul etmek değil, önemli iddiaları yeterli kanıt olmadan doğru kabul etmemektir. Şüphecilik, sonucu önceden belirlemek yerine alternatif açıklamalara açık kalmayı gerektirir.

İlke 13: Yönetim beyanı, politika veya prosedür uygulamanın doğrudan kanıtı sayılmamalıdır.

Bir kuruluşun ne yapması gerektiğini tanımlaması ile gerçekte ne yaptığı farklı olabilir. Denetim, amaçlanan yapı ile fiilî davranış arasındaki farkı ayırt edebilmelidir.

İlke 14: Tek bir ekran görüntüsü veya anlık durum kalıcı çalışma davranışını göstermeyebilir.

Bir yapılandırma veya kontrol belirli anda doğru görünürken başka zamanda farklılaşabilir ya da alternatif yollarla aşılabilir. Kanıt, ileri sürülen iddianın zaman ve davranış boyutuyla uyumlu olmalıdır.

İlke 15: Kanıt yeterliliği belge miktarıyla ölçülmemelidir.

Aynı kaynaktan üretilmiş çok sayıda kayıt tek bir güven varsayımını tekrar ediyor olabilir. Yeterlilik, miktardan çok ilgili iddiayı destekleyen kanıtların niteliği, kapsamı ve gerektiğinde birbirinden bağımsızlığıyla oluşmalıdır.

İlke 16: Kanıtın güvenilirliği kaynağı ve üretildiği koşullarla birlikte değerlendirilmelidir.

Denetlenen tarafın kolayca değiştirebildiği bir kayıt ile bağımsız biçimde oluşmuş kanıt aynı ağırlığa sahip olmayabilir. Kanıtın kim tarafından, hangi sistemle ve hangi koşullarda üretildiği taşıdığı güveni etkiler.

İlke 17: Denetim kanıtı gerektiğinde yeniden izlenebilir olmalıdır.

Denetim sonucunun dayanağı başka yetkin bir kişinin makul ölçüde anlayabileceği biçimde ilişkilendirilebilmelidir. Bunun için gereksiz veri kopyalamak değil, sonucun hangi kanıttan nasıl türetildiğini korumak esastır.

İlke 18: Denetim amacı yeni ve gereksiz bilgi maruziyeti oluşturmamalıdır.

Çalışma kâğıtları hassas veri, sır veya kişisel bilgi içerebilir. Kanıt toplama ihtiyacı, inceleme için gerekli olmayan verilerin sınırsız biçimde kopyalanması ve saklanması anlamına gelmemelidir.

İlke 19: Örnekleme bütün kitle hakkında mutlak kesinlik üretmemelidir.

Bir örneklemin hiçbir istisna göstermemesi bütün işlemlerin doğru olduğu anlamına gelmez; tek bir istisna da mutlaka bütün sürecin aynı biçimde bozuk olduğunu göstermez. Örnek sonucu, seçim yöntemi ve örneklemin sınırları içinde yorumlanmalıdır.

İlke 20: Örnek seçimi yalnızca kolay erişilebilen veya beklenen kayıtlarla sınırlı kalmamalıdır.

Örnekleme gerçek popülasyonu ve önemli riskleri makul biçimde temsil edebilmelidir. Kolaylık, sistematik olarak sorunların daha az görüldüğü alanlara yönelmemelidir.

İlke 21: Denetim kontrolün yalnızca varlığını değil gerçek amacını ve etkisini değerlendirmelidir.

Bir kontrolün uygulanması, hedeflenen riski gerçekten azalttığını göstermez. Denetim, kontrolün neden var olduğunu, gerçek çalışma biçimini ve çevresinden dolaşılabilen yolları birlikte değerlendirebilmelidir.

İlke 22: Kontrol tasarımı ile kontrol işleyişi birbirinden ayrıştırılmalıdır.

İyi tasarlanmış bir kontrol uygulanmıyor olabilir; düzenli uygulanan bir kontrol de yanlış tasarlanmış olabilir. Bu iki zayıflığın nedeni ve sonucu farklı olduğu için aynı değerlendirmeye indirgenmemelidir.

İlke 23: Çok sayıda zayıf veya aynı varsayıma bağlı kontrol güçlü güvence gibi toplanmamalıdır.

Birden fazla kontrol birbirinden bağımsız görünse de aynı veri, kişi veya sistem başarısızlığında birlikte etkisiz hale gelebilir. Denetim kontrol sayısının arkasındaki gerçek bağımsızlığı değerlendirmelidir.

İlke 24: Denetim yalnızca olağan çalışma koşullarını değerlendirmekle yetinmemelidir.

İstisna, acil durum, hata ve alternatif erişim yolları sistemin gerçek güvenlik veya kontrol modelini değiştirebilir. Sadece normal iş akışının incelenmesi sistemin gerçek davranışını eksik gösterebilir.

İlke 25: Bulgu yalnızca beklenen durum ile mevcut durum arasındaki fark olmamalıdır.

Anlamlı bir bulgu sorunun neden önemli olduğunu, hangi güvence iddiasını etkilediğini ve mümkün olduğu ölçüde hangi koşullardan kaynaklandığını ortaya koymalıdır. Belirtiyi raporlamak, sorunu anlamakla aynı şey değildir.

İlke 26: Bulgunun önemi teknik veya biçimsel sınıfından çok gerçek sonuçla ilişkilendirilmelidir.

Aynı kontrol eksikliği farklı alanlarda çok farklı risk oluşturabilir. Derecelendirme, bulgu sayısı veya kontrol türünden çok maruziyet, etki ve ilgili diğer güven unsurlarını dikkate almalıdır.

İlke 27: Denetim dili ne gereksiz dramatizasyon ne de gereksiz yumuşatma üretmelidir.

Rapor, kanıtın desteklediği etkiyi olduğundan büyük göstermemeli; aynı zamanda karar vericilerin önemli bir sorunu gözden kaçırmasına yol açacak biçimde küçümsememelidir. Güven, doğru anlatımdan doğmalıdır.

İlke 28: Denetim önerisi tek bir teknik çözümün dayatılması olmak zorunda değildir.

Denetçinin görevi çoğu durumda hangi risk veya güvence açığının giderilmesi gerektiğini açıklamaktır. Çözüm önerildiğinde bunun kuruluş bağlamına uygunluğu ve oluşturabileceği yeni riskler de dikkate alınmalıdır.

İlke 29: Yönetimin risk kabulü denetim gerçeğini değiştirmemelidir.

Yönetim bilinçli olarak belirli bir riski taşıyabilir; ancak bu karar denetçinin gözlemlediği zayıflığı geriye dönük olarak ortadan kaldırmaz. Risk kabulü ile denetim sonucu ayrı fakat ilişkili karar alanlarıdır.

İlke 30: Görüş ayrılığı gizlenmemelidir.

Denetçi ve yönetim aynı kanıtı farklı yorumlayabilir. Uygun durumlarda bu farkın varlığı, tek bir uzlaşılmış anlatı oluşturmak adına ortadan kaldırılmamalıdır.

İlke 31: Denetim raporu karar vericinin gerçek durumu anlayabileceği açıklıkta olmalıdır.

Teknik ayrıntı gerektiğinde bulunabilir; ancak raporun özü anlaşılmadan kullanılan yöntem ve jargon arasında kaybolmamalıdır. İyi raporlama karmaşık durumu gereksiz biçimde basitleştirmeden anlaşılır kılar.

İlke 32: Denetim sonucu kanıtın desteklediğinden daha fazla kesinlik taşımamalıdır.

Sınırlı test veya örneklem sonucundan tüm sistem hakkında mutlak hüküm üretmek yanlış güvence oluşturur. Olumlu veya olumsuz sonuç, elde edilen kanıtın gerçek kapsam ve kesinlik düzeyiyle uyumlu olmalıdır.

İlke 33: Bulgu bulunmaması otomatik olarak olumlu güvence anlamına gelmemelidir.

Hiçbir sorun görülmemesi iyi bir durum olabilir; fakat kapsam, yöntem veya kanıt zayıfsa aynı sonuç hiçbir şeyin yeterince sınanmadığı anlamına da gelebilir. Güvence bulgu sayısından bağımsız değerlendirilmelidir.

İlke 34: Bulgunun kapatılması yalnızca eylemin tamamlandığı beyanına dayanmamalıdır.

Bir faaliyet yapılmış olsa bile hedeflenen risk azaltılmamış olabilir. Takip, mümkün olduğu ölçüde bulguyu doğuran güvence açığının gerçekten giderilip giderilmediğini değerlendirmelidir.

İlke 35: Tekrarlanan bulgular daha temel yönetişim veya sistem sorununa işaret edebilmelidir.

Benzer sorunların sürekli geri gelmesi yalnızca ilgili birimin gerekli aksiyonu almadığını değil, teşviklerin, sahipliğin veya kontrol yapısının daha temel biçimde yetersiz olduğunu gösterebilir.

İlke 36: Denetim performansı bulgu sayısı veya çalışma süresiyle ölçülmemelidir.

Daha fazla bulgu daha iyi denetim, daha kısa süre de daha verimli güvence anlamına gelmez. Değer, önemli risklerin doğru görülmesi ve karar vericilere güvenilir bilgi sağlanmasıyla ilişkilendirilmelidir.

İlke 37: Denetçi yetkinliği verilen güvence iddiasının karmaşıklığıyla uyumlu olmalıdır.

Bir konunun denetim programında bulunması ekipte onu anlayabilecek yeterli bilgi bulunduğunu göstermez. Uzman desteği kullanılabilir; ancak uzman kullanımı denetçinin ulaştığı sonuç üzerindeki sorumluluğunu ortadan kaldırmamalıdır.

İlke 38: Denetim yöntemleri kullanılan teknoloji ve çalışma biçimleriyle birlikte gelişebilmelidir.

Yeni sistemleri yalnızca eski kanıt ve örnekleme yöntemleriyle değerlendirmek gerçek davranışın önemli bölümlerini kaçırabilir. Yöntem değişirken denetimin temel kanıt, bağımsızlık ve muhakeme ilkeleri korunmalıdır.

İlke 39: Veri analitiği ve yapay zekâ profesyonel muhakemenin sahibi haline gelmemelidir.

Bu araçlar daha geniş veriyi inceleyebilir ve yeni örüntüler ortaya çıkarabilir; ancak sonuçları yanlış, eksik veya bağlamdan kopuk olabilir. Nihai denetim değerlendirmesi kullanılan aracın değil, kanıtı anlayan sorumlu denetimin kararı olmalıdır.

İlke 40: İç denetim kendi güvenilirliğini de sorgulayabilmelidir.

Güvence veren fonksiyonun yöntemleri, bağımsızlığı ve kalitesi sorgulanamaz kabul edilmemelidir. İç denetim de kendi varsayımlarını, kör noktalarını ve gerçek değerini zaman içinde değerlendirebilmelidir.

İlke 41: İç denetim güvencesi gerçek kanıt ve bağımsız muhakeme üzerinden doğrulanabilmelidir.

Planlar, çalışma programları, rapor formatları veya tamamlanmış denetim sayıları tek başına güvence kalitesi oluşturmaz. Önemli iddiaların uygun kanıtla sınandığı, kanıtın sınırlarının dürüst biçimde yansıtıldığı ve sonucun çıkar baskısından bağımsız olarak ifade edilebildiği gösterilebilmelidir.