TRtest
Test ve Değerlendirme A.Ş.

YÖNETİŞİM RİSK UYUMLULUK ÜRÜN GRUBU KRİTERLERİ

No	Başlık/Soru
UG	**1.ÜRÜN GÜVENLİĞİ**
UG_YA	**Yönetim Arayüzleri**
UG_YA_1	Erişim yönetimi ve yetkilendirme yapılıyor mu?
UG_KD	**Kimlik Doğrulama**
UG_KD_1	LDAP, MS AD kimlik doğrulama entegrasyonu destekleniyor mu?
UG_KD_2	Form tabanlı kimlik doğrulama uygulanıyor mu?
UG_KD_3	Parolalar, saklandığı ortamda salted hash formatında mıdır?
UG_KD_4	Parola karmaşıklığı, uzunluk, zaman kısıtlaması mevcut mu?
UG_KD_5	Kullanıcı işlemleri kayıt altına alınıyor mu ?(insert, update, delete, kimlik)
UG_VK	**Veri Koruma**
UG_VK_1	Veri giriş alanlarında (tehlikeli karakter, uzunluk, tür gibi) kısıt uygulanabiliyor mu?
UG_VK_2	Çıktı kodlama yapılıyor mu?
UG_B	**Bağımlılıklar**
UG_B_1	Çoklu dil desteği (multilanguage support) var mı?
UG_B_2	Yetkilendirmede kullanıcı veya rol bazlı yetkilendirme yapabiliyor mu?
UG_B_3	Uygulamanın yönetimsel ayarlarının değiştirilebilmesi için bir yönetim menusu bulunuyor mu?
UG_B_4	Kullanıcı şifreleri tanımlanabiliyor ve sıfırlanabiliyor mu?
TO	**2.TEMEL ÖZELLİKLER**
TO_Y	**Yetkilendirme**
TO_Y_1	Ön tanımlı yetki grupları kullanılıyor mu?
TO_M	**Mimari**
TO_M_1	Varlık, süreç, risk sonuçları herhangi bir formatta(örneğin; PDF, XLSX, DOCX, CSV, HTML formatlarından en az birinde) dışarıya aktarabiliyor mu?
TO_M_2	Oturum zaman aşımı (idle time out) yapılıyor mu?

TO_OB	**Organizasyonun Bağlamı**
TO_OB_1	Yönetim organizasyonu uygulama üzerinde tanımlanabiliyor mu?
TO_DFY	**Düzeltici Faaliyet Yönetimi**
TO_DFY_1	Uygunsuzluklar için minimum veri alanları (örnek;uygunsuzluk nedeni, alınacak aksiyon, kapanış tarihi, sorumlusu, kök neden) tanımlanabiliyor mu?
TO_DFY_2	Uygunsuzluğun bildirilmesinin ardından tespit edilen birim yöneticisi çözüm ekibi lideri ve kullanıcı veya kullanıcı grubu belirleyerek uygunsuzluk onayını uygulama aracılığı ile verebiliyor mu?
TO_DFY_3	Uygunsuzlukla ilgili tüm aksiyonlar tamamlandıktan sonra uygunsuzluk kontrol sorumlusuna bildirim otomatik olarak yapılıyor mu?
TO_DFY_4	Kontrol sorumlusunun değerlendirmesine bağlı olarak uygunsuzluk kapatılıyor mu ya da birim sorumlusuna kapanış değerlendirme bilgisi ile birlikte e-posta ile bildirim yapılıyor mu?
TO_AY	**Aksiyon Yönetimi**
TO_AY_1	Uygulama üzerinden aksiyon tanımlaması yapılabiliyor mu?
TO_AY_2	Aksiyon tanımlamasında aksiyon sorumlusu onayı seçeneği sağlanıyor mu?
TO_AY_3	Aksiyon planlamasından minimum alanlar (aksiyon sorumlusu, açıklaması, planlanan tamamlanma tarihi, etkinlik değerlendirme sorumlusu) tanımlanabiliyor mu?
TO_IOY	**İhlal Olayları Yönetimi**
TO_IOY_1	İhlal bildirimleri yapılabiliyor mu?
TO_IOY_2	İhlal olaylarında uygulama aracılığı ile ilgili ihlal olaylarını yönetecek kişiye otomatik bilgilendirme yapılabiliyor mu?
TO_G	**Genel**
TO_G_1	Toplam varlık sayısı, risk analizi yapılmamış varlık sayısı, açık DF sayısı, açık aksiyon sayısı, ihlâl olayı sayıları özet olarak gösterilebiliyor mu?
TO_G_2	TS EN ISO/IEC 27001 Standardına ilişkin kontrol maddeleri tanımlanabiliyor ve güncellenebiliyor mu?
TO_G_3	Standarttakilere ilave kontrol maddesi tanımlanabiliyor mu?
TO_G_4	Uygulama kullanım esnasında yardım menüleri sunuyor mu?
TO_G_5	Uygulama üzerinden kurumun iş süreçleri tanımlanabiliyor mu?
TO_G_6	Doküman ve varlıkların sınıflandırılması için kurumsal bazda kullanılan gizlilik dereceleri tanımlanabiliyor ve bunlar doküman ve varlıklara atanabiliyor mu?
TO_G_7	İş süreçleri ile varlıklar ilişkilendirilebilir mi?
TO_R	**Risk Yönetimi**
TO_R_1	Risklerin tanımlanmasına, analizine ve önceliklendirilmesine imkan tanıyor mu?
TO_R_2	Risklere erişim yetki bazlı mı? (Örnek: Tüm risklerin tüm kullanıcılar tarafından görüntülenememesi)
TO_R_3	Risk durumu değişimine göre risk durumu iyileştiği bir puanlama sistemi ile gösteriliyor mu?

TO_R_4	Risk analizi, süreçler ile ilişkilendirilebiliyor mu?
TO_RAY	**Risk Analizi ve Yönetimi**
TO_RAY_1	Varlık ve varlık kategorileri tanımlanabiliyor mu?
TO_RAY_2	Yazılım hazır varlık kategorileri sağlıyor ve değişiklikler yapılmasına izin veriyor mu?
TO_RAY_3	Varlık sahipliği organizasyon şemasından seçilebiliyor mu? Organizasyondaki birimlerin varlık sahipliklerine atanması sırasında ilgili birimi arama özellikleri mevcut mudur?
TO_RAY_4	Tanımlanan varlıklarla bir envanter oluşturulabiliyor ve raporlar alınabiliyor mu?.
TO_RAY_5	Varlıklara ait yer bilgisi girilebiliyor mu?
TO_RAY_6	Varlıklar için ad ve açıklama girilebiliyor mu?
TO_RAY_7	Varlık değeri gizlilik, bütünlük, erişilebilirlik için üç farklı değer olarak girilebiliyor mu?
TO_RAY_8	Varlıklar için sınıflandırma seçilebiliyor mu?
TO_RAY_9	Varlıklara ikincil iş sahipliği veya emanetçi atanabiliyor mu?
TO_RAY_10	Kategoriye atanan riskler kategorideki tüm varlıklarla ya da seçilen varlıklarla otomatik olarak ilişkilendiriliyor mu?
TO_RAY_11	Tehditler ve tehdit kategorileri tanımlanabiliyor mu?
TO_RAY_12	Tehditler için zafiyetler tanımlanabiliyor mu?
TO_RAY_13	Kabul edilebilir risk seviyeleri tanımlanabiliyor ve değiştirilebiliyor mu? Bu seviyenin üzerindeki riskler farklı bir renkte (ör. Kırmızı) ile gösterilebiliyor mu?.
TO_RAY_14	Uygulama üzerinden varlık sahipliği toplu bir şekilde değiştirilebiliyor mu?
TO_RAY_15	Tespit edilen riskler için aksiyon veya DF planlanıp, riskin sahipleri belirlenip takip edilebiliyor mu?
TO_RAY_16	Aksiyonlar ve DF istekleri risk sahiplerine ve yöneticiye otomatik olarak ve e-posta yoluyla iletilebiliyor mu?
TO_RAY_17	Risk Değerlendirme ve Risk İyileştirme Raporları alınabiliyor mu?
TO_RAY_18	Raporlar bilgi girişi yapılan tüm alanlar bazında filtrelenerek alınabiliyor mu?
TO_RBVY	**Risk ve Bilgi Varlık Yönetimi**
TO_RBVY_1	Risk tanımlamasında minimum alanlar (varlık, süreç, bölüm, risk adı, risk açıklaması,riskin sahibi, risk seviyesi) karşılanıyor mu?
TO_RBVY_2	Risk analizinde minimum alanlar (Gerçekleşme olasılığı, etki seviyesi, risk seviyesi) karşılanıyor mu?
TO_RBVY_3	Risk işleme seçenekleri azaltma,transfer, kaçınma, kabul işlemlerine göre riskin durumu belirlenebiliyor mu?
TO_IDDY	**İç / Dış Denetim Yönetimi**
TO_IDDY_1	Birden fazla denetimi içeren denetim programları tanımlanabiliyor mu?
TO_IDDY_2	Denetim planları minimum alanları (denetimin tanımı, amacı, kapsamı, kriterleri, denetim takımı, başlangıç ve bitiş zamanı, detaylı iş planı) tanımlanabiliyor mu?

TO_IDDY_3	Denetim soru listeleri uygulama aracılığı ile oluşturulabiliyor mu?
TO_IDDY_4	Denetimler belli periyotlarda yapılması ve raporlanabilmesi sağlanır mı?
TO_DY	**Doküman Yönetimi**
TO_DY_1	Uygulamada dokümanlar ve versiyonları takip edilebiliyor mu?
TO_DY_2	Dokümanlar için politika, prosedür, standart vb. şekilde doküman türleri tanımlanabiliyor mu?
TO_DY_3	Dokümanlara yetki kısıtlaması ile erişilebiliyor mu?
TO_KYEO	**Kullanıcı Yönetimi ve Entegrasyon Özellikleri**
TO_KYEO_1	Yerel kullanıcı ve/veya grup eklenebiliyor mu?
TO_RO	**Raporlama Özellikleri**
TO_RO_1	Default şablonlar (risk analizi, varlık listesi vb.) ile hızlı rapor alınabiliyor mu ?
TO_RO_2	Uygulama üzerinden güncel doküman listesi alınabiliyor mu?
TO_RO_3	Raporlar menülerden seçilerek görüntülenebiliyor mu?
TO_RO_4	Uygulamada aşağıdaki raporlar tanımlı mı ve menüden raporlara ulaşılabiliyor mu?
TO_RO_5	▪Risk Raporu – Risk Seviyesi ortalama olarak ve ayrıca Gizlilik, Bütünlük, Erişilebilirlik için ayrı ayrı gösterilebilmelidir.
TO_RO_6	▪ S.O.A (Statement of Applicability) Raporu
TO_RO_7	▪Varlık Envanteri Raporu
TO_RO_8	▪Tehdit Raporu
TO_RO_9	▪Risk İşleme Raporu
TO_RO_10	▪Sahiplerine Göre Varlıklar
TO_RO_11	▪Değerlerine Göre Varlıklar
TO_RO_12	▪Değerlerine Göre Riskler
TO_UD	**Ürün Dokümantasyonu**
TO_UD_1	Ürün dokümantasyonu var mıdır?(Yazılı materyal veya Tool Tip vb.)
TO_OY	**Organizasyon Yönetimi**
TO_OY_1	Organizasyon (birimler), kullanıcılar web ara-yüzü ile tanımlanabiliyor mu?
TO_OY_2	Kullanıcılar için yetkilerine göre gruplar yaratılabiliyor ve kullanıcılar bu gruplara atanabiliyor mu? (yetkisiz kullanıcı, yönetici, vb.)
TO_OY_3	Organizasyon bilgisinin güncellenmesi elle (manuel) ya da otomatik olarak gerçekleştirilebiliyor mu?

TO_OIY	**Olay / İhlal Yönetimi**
TO_OIY_1	Uygulamada güvenlik olaylarını kayıt ve takip edebilmek için bir olay /ihlal yönetim modülü bulunuyor mu?
TO_OIY_2	Olay bildirimleri ve sisteme girişleri uygulama üzerinden gerçekleştirilebiliyor mu?
TO_OIY_3	Olay sisteme girildikten sonra alınması gereken aksiyonlar ve bu aksiyonları gerçekleştirecek kişi ya da organizasyon birimi uygulamada tanımlanabiliyor ve aksiyonun takibi yapılabiliyor mu?
TO_OIY_4	Kullanıcı tarafından bildirilen olaylar listelenebiliyor mu?
TO_OIY_5	Kullanıcıya yönlendirilen olaylar listelenebiliyor mu?
TO_OIY_6	Olay /İhlal raporu alınabiliyor mu?
TO_OIY_7	Olay bildirimi ile birlikte düzeltici faaliyet tanımı yapılabiliyor mu ?
TO_YGG	**YGG Toplantı Yönetimi**
TO_YGG_1	Uygulama üzerinden toplantı planlanıp, katılımcılar, gündem belirlenebiliyor mu?