D-Tek Bilgi Merkezi

ISO/IEC 42001:2023 Bilgi Teknolojisi-Yapay Zeka-Yönetim Sistemi Standardı Özeti

Prof. Dr. Diler Aslan

D-Tek Teknoloji Geliştirme, Üretim, Eğitim ve Danışmanlık Hizmetleri Ltd. Şti.

Yayın tarihi	30.08.2026
Son güncelleme	30.08.2026
Doküman sürüm	00

ISO/IEC 42001:2023 Bilgi Teknolojisi-Yapay Zeka-Yönetim Sistemi Standardı Özeti

Prof. Dr. Diler Aslan
30.08.2026

İçindekiler

Bu standart Kuruluşta Yapay Zekâ Sistemlerinin Yönetimi ile ilgili önerilerde bulunur.

ISO/IEC 42001:2023, Information technology — Artificial intelligence — Management system, kuruluşların yapay zekâ sistemlerini sorumlu biçimde geliştirmesi, sağlaması veya kullanması için hazırlanmış bir yönetim sistemi standardıdır.

Standart, bir **Yapay Zekâ Yönetim Sisteminin (Artificial Intelligence Management System – AIMS)** kurulması, uygulanması, sürdürülmesi ve sürekli iyileştirilmesi için şartları belirler. Her büyüklükteki kamu, özel ve kâr amacı gütmeyen kuruluşa uygulanabilir. Yapay zekâ geliştiren kuruluşların yanında yapay zekâ kullanan kuruluşları da kapsar.

Standardın amacı

ISO/IEC 42001'in temel amacı, kuruluşun yapay zekâ sistemlerini:

- Kuruluşun amaçlarıyla uyumlu,
- Yasal ve düzenleyici şartlara uygun,
- Etik ve sorumlu,
- Şeffaf ve izlenebilir,
- Güvenli ve güvenilir,
- İnsan gözetimi altında,
- Riskleri ve etkileri değerlendirilmiş,
- Yaşam döngüsü[1] boyunca kontrol edilen

bir yapıda yönetmesini sağlamaktır.

Standart, belirli bir **yapay zekâ sisteminin teknik doğruluğunu gösteren** bir ürün standardı **değildir**. Kuruluşun yapay zekâya ilişkin **politikasını, yönetişimini, süreçlerini, sorumluluklarını ve kontrollerini** düzenler.

Yönetim sistemi şartları

ISO/IEC 42001, diğer ISO yönetim sistemi standartları gibi 4–10. maddelerden oluşan ortak yapıyı kullanır.

4. Kuruluşun bağlamı

Kuruluş, yapay zekâ yönetim sistemini etkileyebilecek iç ve dış konuları belirlemelidir.

Bunlar arasında:

- Kuruluşun amaçları ve faaliyetleri
- Kullandığı veya geliştirdiği yapay zekâ sistemleri
- Yasal ve düzenleyici şartlar
- Teknolojik gelişmeler
- Etik ve toplumsal beklentiler
- Veri ve altyapı koşulları

[1] Bkz. Yapay Zeka Sistemi Yaşam Döngüsü Dosyası

- Yapay zekâdan etkilenen kişi ve gruplar

bulunur.

Kuruluş aynı zamanda ilgili tarafları ve onların gereksinimlerini belirlemeli, yapay zekâ yönetim sisteminin kapsamını tanımlamalıdır.

5. Liderlik

Üst yönetim, yapay zekâ yönetim sisteminin kurulması ve etkinliğinden sorumludur.

Üst yönetim:

- Yapay zekâ politikasını oluşturmalı,
- Yönetim sistemini kuruluşun süreçleriyle bütünleştirmeli,
- Gerekli kaynakları sağlamalı,
- Sorumlu yapay zekâ kullanımını desteklemeli,
- Görev, yetki ve sorumlulukları tanımlamalı,
- Sürekli iyileştirmeyi teşvik etmelidir.

Yapay zekâ politikası

Politika:

- Kuruluşun amaçlarına uygun olmalı,
- Yapay zekâ hedefleri için çerçeve sağlamalı,
- Uygulanabilir şartlara uyma taahhüdünü içermeli,
- Sorumlu yapay zekâ kullanımını desteklemeli,
- Sürekli iyileştirme taahhüdü taşımalıdır.

6. Planlama

Planlama aşamasının temel bileşenleri şunlardır:

Yapay zekâ risk ve fırsatların belirlenmesi

Kuruluş:

- Risk değerlendirme yöntemini tanımlamalı,
- Yapay zekâya ilişkin riskleri belirlemeli,
- Risklerin olasılık ve sonuçlarını değerlendirmeli,
- Risklerin kabul edilebilirliğine karar vermeli,
- Risklerin önceliklerini belirlemelidir.

Riskler yalnız teknik arızaları değil, örneğin:

- Yanlılık ve adil olmayan sonuçları,

- Açıklanabilirlik eksikliğini,
- Hatalı veya yanıltıcı çıktıları,
- Kişisel verilerin korunmasını,
- Güvenliği,
- İnsanların yapay zekâya aşırı güvenmesini,
- Amaçlanan kullanım dışında kullanımı,
- Bireyler ve toplum üzerindeki olumsuz etkileri

de kapsayabilir.

Risklerin işlenmesi (Risk Treatment)

Kuruluş, belirlenen riskler için kontrol önlemleri seçmeli ve bir risk işleme planı hazırlamalıdır.

Ek A'daki kontrollerle karşılaştırma yapılarak:

- Gerekli kontroller,
- Uygulanmayan kontroller ve bunların gerekçeleri,
- Kuruluşun eklediği diğer kontroller

belirlenir.

Bunlar **Uygulanabilirlik Bildirgesi'nde (Statement of Applicability)** gösterilir[2].

Yapay zekâ sistemi etki değerlendirmesi

Standart, risk değerlendirmesinin yanında **YZ sistemi etki değerlendirmesi** yapılmasını da ister.

Bu değerlendirmede yapay zekâ sisteminin:

- Bireyler,
- Kişi grupları,
- Çalışanlar,
- Müşteriler veya hizmet alanlar,
- Toplum

üzerindeki olası sonuçları ele alınır.

[2] Bkz. "Uygulanabilirlik Tanımı ve Diğer Dokümanlarla İlişkiler" ve "Yapay Zekâ Sistemi Uygulanabilirlik Bildirgesi Dokumani Ornegi" Dosyaları

Risk değerlendirmesi ile etki değerlendirmesi ilişkilidir; ancak aynı değildir. Risk değerlendirmesi kuruluşun amaçlarını ve faaliyetlerini de kapsarken etki değerlendirmesi, yapay zekâdan etkilenen taraflara yönelir.

Yapay zekâ hedefleri

Kuruluş ölçülebilir yapay zekâ hedefleri belirlemeli; hedefler için sorumluları, kaynakları, zamanlamayı ve değerlendirme yöntemlerini tanımlamalıdır.

7. Destek

Kuruluş, yapay zekâ yönetim sistemi için gerekli:

- İnsan kaynağını,
- Teknik ve mali kaynakları,
- Veri ve bilgi kaynaklarını,
- Altyapıyı,
- Yetkinlikleri

sağlamalıdır.

Yetkinlik ve farkındalık

Yapay zekâ sistemleriyle ilgili kişilerin:

- Eğitimleri,
- Deneyimleri,
- Teknik yeterlilikleri,
- Etik ve risk farkındalıkları,
- Görevlerine ilişkin yetkinlikleri

belirlenmeli ve kanıtlanmalıdır.

Çalışanlar yapay zekâ politikasını, kendi sorumluluklarını ve şartlara uymamanın sonuçlarını bilmelidir.

İletişim

Kuruluş, yapay zekâ konusunda:

- Ne zaman,
- Kiminle,
- Hangi bilginin,
- Kim tarafından,
- Nasıl

paylaşılacağını belirlemelidir.

Dokümante edilmiş bilgi

Kuruluş:

- Standardın istediği dokümanları,
- Yönetim sisteminin etkinliği için gerekli gördüğü dokümanları,
- Yapılan faaliyetleri kanıtlayan kayıtları

oluşturmalı ve kontrol etmelidir.

8. Operasyon

Kuruluş, yapay zekâ sistemlerinin geliştirilmesi, sağlanması veya kullanılmasıyla ilgili süreçleri planlamalı ve kontrol etmelidir.

Operasyon aşamasında:

- Risk değerlendirmesi uygulanır ve güncellenir.
- Risk işleme planı yürütülür.
- Yapay zekâ sistemi etki değerlendirmesi yapılır ve güncellenir.
- Dışarıdan sağlanan süreç, ürün ve hizmetler kontrol edilir.
- Planlanan değişiklikler yönetilir.
- Beklenmeyen değişikliklerin sonuçları değerlendirilir.

Bir yapay zekâ sistemi veya kullanım koşulları değiştiğinde risk ve etki değerlendirmelerinin yeniden yapılması gerekebilir.

9. Performans değerlendirmesi

Kuruluş, yapay zekâ yönetim sisteminin etkinliğini değerlendirmelidir.

İzleme, ölçme, analiz ve değerlendirme

Kuruluş:

- Nelerin izleneceğini,
- Kullanılacak yöntemleri,
- İzleme sıklığını,
- Sonuçların kim tarafından değerlendirileceğini,
- Kayıtların nasıl saklanacağını

belirlemelidir.

Burada değerlendirilen, tek başına model performansı değil, **YZ yönetim sisteminin etkinliğidir**.

İç tetkik

İç tetkiklerle yönetim sisteminin:

- Kuruluşun kendi şartlarına,
- ISO/IEC 42001 şartlarına,
- Belirlenen politika ve süreçlere

uygunluğu ve etkin biçimde uygulanıp uygulanmadığı değerlendirilir.

Yönetimin gözden geçirmesi

Üst yönetim belirli aralıklarla:

- Önceki kararların durumunu,
- İç ve dış değişiklikleri,
- Yönetim sistemi performansını,
- Risk ve etki değerlendirmelerini,
- İç tetkik sonuçlarını,
- Uygunsuzlukları,
- İlgili tarafların geri bildirimlerini,
- Kaynak gereksinimlerini,
- İyileştirme fırsatlarını

gözden geçirmelidir.

10. İyileştirme

Kuruluş, iyileştirme fırsatlarını belirlemeli ve yapay zekâ yönetim sistemini sürekli geliştirmelidir.

Bir uygunsuzluk ortaya çıktığında:

- Uygunsuzluk kontrol altına alınmalı,
- Sonuçları giderilmeli,
- Nedeni araştırılmalı,
- Benzer uygunsuzlukların bulunup bulunmadığı değerlendirilmeli,
- Düzeltici faaliyet uygulanmalı,
- Faaliyetin etkinliği değerlendirilmeli,
- Gerekirse riskler, etkiler ve yönetim sistemi değiştirilmelidir.

Ek A. Referans Kontrol Amaçları ve Kontroller (Normatif)

“Annex A (normative) — Reference control objectives and controls”

Ek A, kuruluşun amaçlarına ulaşması ve YZ sistemlerinin tasarımı, geliştirilmesi, sağlanması ve kullanılmasından kaynaklanan riskleri ele alması için referans kontrol amaçlarını ve kontrolleri içerir.

Ek A, kuruluşun risk işleme sürecinde değerlendireceği **38 kontrolü dokuz başlık altında** toplar. Ana başlıklar:

Ek A	Kontrol alanı	Temel içerik
A.2	Yapay zekâ politikaları	YZ politikasının oluşturulması ve diğer politikalarla uyumu
A.3	İç organizasyon	Görevler, sorumluluklar, olayların bildirilmesi
A.4	YZ sistemleri için kaynaklar	Veri, araçlar, donanım, yazılım, insan kaynağı ve sistem bileşenleri
A.5	YZ sistemi etkilerinin değerlendirilmesi	Etki değerlendirme süreci ve kayıtları
A.6	YZ sistemi yaşam döngüsü	Sorumlu geliştirme, gereksinimler, tasarım, doğrulama, kullanıma alma, işletme ve izleme
A.7	YZ sistemleri için veri	Veri edinme, kalite, köken, hazırlama ve yönetim
A.8	İlgili taraflara bilgi sunulması	Şeffaflık, kullanıcı bilgileri, olayların ve etkilerin bildirilmesi
A.9	YZ sistemlerinin kullanımı	Sorumlu kullanım, kullanım amaçları ve işletim kontrolleri
A.10	Üçüncü taraf ve müşteri ilişkileri	Tedarikçiler, müşteriler ve diğer taraflarla sorumluluk paylaşımı

Kuruluş bütün kontrolleri otomatik olarak uygulamak zorunda değildir. Gerekli kontroller risk ve etki değerlendirmelerine göre seçilir; uygulanmayan kontroller gerekçelendirilir.

A.1 Genel

Ek A'daki bütün kontrollerin her kuruluş tarafından uygulanması gerekmez. Kuruluş, YZ risk değerlendirmesi ve risk işleme sonuçlarına göre gerekli kontrolleri seçer. Seçilen ve dışlanan kontroller ile bunların gerekçeleri **Uygulanabilirlik Bildirgesi**'nde gösterilir (Bkz. Uygulanabilirlik Bildirgesi ile ilgili dosyalar).

Ek A'daki kontroller kapsamlı olmakla birlikte tüketici değildir. Kuruluş, kendi bağlamına ve risklerine göre farklı veya ek kontroller belirleyebilir. Kontrollerin uygulanmasına ilişkin rehberlik Ek B'de verilmektedir.

A.2 YZ ile ilgili politikalar

A.2.2 YZ politikası
A.2.3 Kuruluşun diğer politikalarıyla uyum
A.2.4 YZ politikasının gözden geçirilmesi

Kuruluş, YZ sistemlerinin geliştirilmesi ve kullanılması için bir YZ politikası oluşturmalı ve dokümante etmelidir. Bu politika; kuruluşun amaçları, iş stratejisi, değerleri, risk yaklaşımı ve uygulanabilir gerekliliklerle uyumlu olmalıdır.

YZ politikası; kalite, risk yönetimi, bilgi güvenliği, mahremiyet, insan kaynakları ve diğer ilgili kuruluş politikalarıyla ilişkilendirilmelidir. Politika, uygunluğunu, yeterliliğini ve etkinliğini korumak amacıyla planlı aralıklarla ve önemli değişikliklerden sonra gözden geçirilmelidir.

A.3 İç organizasyon

A.3.2 YZ ile ilgili görev ve sorumluluklar
A.3.3 Kaygıların bildirilmesi

YZ sistemleriyle ilgili görevler, yetkiler ve sorumluluklar kuruluşun gereksinimlerine göre tanımlanmalı, atanmalı ve ilgililere bildirilmelidir. YZ sisteminin sahibi, süreç sahibi, risk sahibi, veri sorumlusu, teknik sorumlu, kullanıcı ve insan gözetimini sağlayan kişiler açıkça belirlenmelidir.

Çalışanların ve diğer ilgili kişilerin YZ sistemleriyle ilgili hata, uygunsuzluk, etik sorun veya diğer kaygıları bildirebileceği bir süreç oluşturulmalıdır. Bildirimlerin gizlilik içinde yapılabilmesi ve gerektiğinde üst yönetime iletilebilmesi sağlanmalıdır.

A.4 YZ sistemleri için kaynaklar

A.4.2 Kaynakların dokümantasyonu
A.4.3 Veri kaynakları
A.4.4 Araç kaynakları
A.4.5 Sistem ve hesaplama kaynakları
A.4.6 İnsan kaynakları

YZ sisteminin yaşam döngüsü boyunca gerekli kaynaklar belirlenmeli ve dokümante edilmelidir. Kaynaklar; veri, algoritma, model, yazılım araçları, geliştirme ve test ortamları, donanım, ağ, depolama ve hesaplama altyapısını kapsar.

YZ sistemiyle ilgili görevleri yürütecek kişilerin gerekli bilgi, eğitim, deneyim ve yetkinlikleri belirlenmelidir. Kaynakların yeterliliği, sistemde veya kullanım koşullarında değişiklik olduğunda yeniden değerlendirilmelidir.

A.5 YZ sistemlerinin etkilerinin değerlendirilmesi

A.5.2 YZ sistemi etki değerlendirmesi süreci
A.5.3 YZ sistemi etki değerlendirmelerinin dokümantasyonu

A.5.4 YZ sisteminin bireyler veya birey grupları üzerindeki etkilerinin değerlendirilmesi

A.5.5 YZ sistemlerinin toplumsal etkilerinin değerlendirilmesi

Kuruluş, YZ sistemlerinin bireyler, birey grupları ve toplum üzerindeki olası olumlu ve olumsuz etkilerini değerlendirmek için bir süreç oluşturmalıdır.

Değerlendirmede sistemin amacı, kullanım ortamı, otomasyon düzeyi, kullanılan veriler, insan gözetimi, sağlık ve güvenlik, temel haklar, mahremiyet, hakkaniyet, erişilebilirlik ve toplumsal etkiler dikkate alınmalıdır.

Etki değerlendirmesinin yöntemi, bulguları ve alınan kararlar dokümante edilmelidir. Değerlendirme, sistemde veya kullanım bağlamında önemli bir değişiklik olduğunda güncellenmelidir.

A.6 YZ sistemi yaşam döngüsü

A.6.1 YZ sisteminin geliştirilmesine ilişkin yönetim rehberliği

A.6.1.2 YZ sisteminin sorumlu geliştirilmesine ilişkin amaçlar

A.6.1.3 YZ sistemlerinin sorumlu tasarım ve geliştirme süreçleri

Kuruluş, YZ sistemlerinin sorumlu biçimde geliştirilmesine ilişkin amaçları belirlemelidir. Bu amaçlar kuruluşun YZ politikası, risk ölçütleri, ilgili tarafların gereksinimleri ve YZ sistemi etki değerlendirmesiyle uyumlu olmalıdır.

Sorumlu geliştirme ilkelerinin tasarım ve geliştirme süreçlerine nasıl yerleştirileceği tanımlanmalıdır. Tasarım kararları, sorumlular, kontrol noktaları ve onay mekanizmaları belirlenmelidir.

A.6.2 YZ sistemi yaşam döngüsü

A.6.2.2 YZ sistemi gereksinimleri ve özellikleri

A.6.2.3 YZ sistemi tasarım ve geliştirmesinin dokümantasyonu

A.6.2.4 YZ sisteminin doğrulanması ve geçerli kılınması

A.6.2.5 YZ sisteminin kullanıma alınması

A.6.2.6 YZ sisteminin işletilmesi ve izlenmesi

A.6.2.7 YZ sistemi teknik dokümantasyonu

A.6.2.8 YZ sisteminin olay günlüklerini kaydetmesi

YZ sisteminin gereksinimleri ve özellikleri, amaçlanan kullanım ve sorumlu geliştirme amaçları doğrultusunda belirlenmelidir. Tasarım ve geliştirme kararları izlenebilir biçimde dokümante edilmelidir.

Sistemin belirtilen gereksinimleri karşıladığı doğrulanmalı; amaçlanan kullanım ortamında beklenen sonucu sağlayabildiği geçerli kılınmalıdır. Kullanıma alma öncesinde kabul ölçütleri, gerekli onaylar, kullanıcı hazırlığı ve geri dönüş planları belirlenmelidir.

Canlı kullanımda sistem performansı, veri ve model sapması, insan müdahaleleri, olaylar ve kullanım sınırlarına uyum izlenmelidir. Teknik dokümantasyon güncel tutulmalı ve gerekli sistem olayları kaydedilmelidir.

A.7 YZ sistemleri için veri

- **A.7.2 YZ sisteminin geliştirilmesi ve iyileştirilmesi için veri**
- **A.7.3 Verinin edinilmesi**
- **A.7.4 YZ sistemleri için veri kalitesi**
- **A.7.5 Veri kökeni**
- **A.7.6 Verinin hazırlanması**

YZ sisteminin geliştirilmesi, eğitilmesi, doğrulanması, test edilmesi, kullanılması ve iyileştirilmesi için gerekli veriler tanımlanmalıdır. Eğitim, doğrulama ve test verilerinin kullanım amaçları birbirinden ayrılmalıdır.

Verinin kaynağı, edinme yöntemi, hukuki dayanağı, izinleri ve kullanım kısıtları belirlenmelidir. Veri kalitesi; doğruluk, tamlık, tutarlılık, güncellik, temsil gücü ve amaca uygunluk bakımından değerlendirilmelidir.

Verinin kökeni ve geçirdiği işlemler izlenebilir olmalıdır. Temizleme, dönüştürme, birleştirme, etiketleme ve özellik çıkarma gibi veri hazırlama işlemleri tanımlanmalı ve dokümante edilmelidir.

A.8 YZ sistemleriyle ilgili taraflara sunulan bilgiler

- **A.8.2 Sistem dokümantasyonu ve kullanıcılara sunulan bilgiler**
- **A.8.3 Dış bildirim**
- **A.8.4 Olayların iletişimi**
- **A.8.5 İlgili taraflara sunulan bilgiler**

Kullanıcılara YZ sisteminin amacı, amaçlanan kullanımı, kullanım sınırları, performansı, bilinen riskleri, gerekli insan gözetimi ve kullanım talimatları hakkında yeterli bilgi sunulmalıdır.

Mevzuat, sözleşmeler veya kuruluş politikaları gereğince yapılacak dış bildirimler için bir süreç oluşturulmalıdır. YZ sistemi olaylarının kullanıcılara, müşterilere, yetkili kurumlara ve diğer ilgili taraflara ne zaman, kim tarafından ve nasıl bildirileceği belirlenmelidir.

İlgili taraflara sunulan bilgiler, tarafların gereksinimlerine uygun, anlaşılır, erişilebilir ve güncel olmalıdır.

A.9 YZ sistemlerinin kullanılması

A.9.2 YZ sistemlerinin sorumlu kullanımına ilişkin süreçler
A.9.3 YZ sisteminin sorumlu kullanımına ilişkin amaçlar
A.9.4 YZ sisteminin amaçlanan kullanımı

Kuruluş, YZ sistemlerinin sorumlu biçimde kullanılması için süreçler ve amaçlar belirlemelidir. Bu süreçler; insan gözetimi, çıktıların değerlendirilmesi, kullanım sınırları, sapmaların yönetimi ve gerektiğinde kullanımın durdurulmasını kapsamalıdır.

YZ sistemi, tanımlanan amaçlanan kullanım ve üretici veya sağlayıcı tarafından sunulan dokümantasyon doğrultusunda kullanılmalıdır. Sistemin kimler tarafından, hangi amaçla, hangi koşullarda ve hangi sınırlar içinde kullanılacağı açıkça belirlenmelidir.

Amaç dışı veya uygun olmayan kullanımın önlenmesi için teknik ve yönetsel kontroller uygulanmalıdır.

A.10 Üçüncü taraf ve müşteri ilişkileri

A.10.2 Sorumlulukların dağıtılması
A.10.3 Tedarikçiler
A.10.4 Müşteriler

YZ sistemi yaşam döngüsünde kuruluş, geliştirici, tedarikçi, veri sağlayıcı, müşteri ve diğer üçüncü taraflar arasındaki görev ve sorumluluklar açıkça belirlenmelidir.

Sorumluluk dağılımı; risklerin yönetimi, kontrollerin uygulanması, performansın izlenmesi, değişikliklerin yönetimi, olayların bildirilmesi ve gerekli bilgilerin paylaşılmasını kapsamalıdır.

Tedarik edilen veri, model, yazılım, araç, hizmet veya YZ sisteminin kuruluşun sorumlu YZ yaklaşımına uygunluğu değerlendirilmelidir. Müşterilere sistemin amaçlanan kullanımı,

kullanım sınırları, bilinen riskleri ve kendilerine düşen sorumluluklar hakkında yeterli bilgi sağlanmalıdır.

Ek B. Yapay Zeka Kontrollerinin Uygulanması Rehberi (Bilgilendirici)

Annex B (normative) — Implementation guidance for AI controls
Ek A kontrollerinin uygulanmasına ilişkin rehberlik sağlar.

B.1 Genel

Ek A'daki kontrollerin nasıl uygulanabileceğini açıklar. Buradaki uygulama rehberinin Uygulanabilirlik Bildirgesi'nde ayrı ayrı gerekçelendirilmesi gerekmez. Kuruluş, kendi bağlamına ve risklerine göre rehberliği genişletebilir veya farklı kontroller geliştirebilir.

B.2 YZ ile ilgili politikalar

- **B.2.1 Amaç**
- **B.2.2 YZ politikası**
- **B.2.3 Diğer kuruluş politikalarıyla uyum**
- **B.2.4 YZ politikasının gözden geçirilmesi**

Kuruluşun YZ geliştirme ve kullanım politikasının iş stratejisi, değerleri, risk yaklaşımı, mevzuat ve ilgili tarafların beklentileriyle uyumlu olması gerekir. YZ politikası; kalite, güvenlik, bilgi güvenliği, gizlilik ve diğer kurumsal politikalarla ilişkilendirilmeli ve düzenli olarak gözden geçirilmelidir.

B.3 İç organizasyon

- **B.3.1 Amaç**
- **B.3.2 YZ ile ilgili görev ve sorumluluklar**
- **B.3.3 Kaygıların bildirilmesi**

YZ sistemi yaşam döngüsündeki görev, yetki ve sorumlulukların tanımlanmasını ister. Çalışanların YZ sistemleriyle ilgili kaygı, hata veya etik sorunları gizlilik içinde bildirebileceği ve gerektiğinde üst yönetime taşıyabileceği bir mekanizma kurulmalıdır.

B.4 YZ sistemleri için kaynaklar

- **B.4.1 Amaç**
- **B.4.2 Kaynakların dokümantasyonu**
- **B.4.3 Veri kaynakları**
- **B.4.4 Araç kaynakları**
- **B.4.5 Sistem ve hesaplama kaynakları**
- **B.4.6 İnsan kaynakları**

YZ sisteminin geliştirilmesi, kullanılması ve izlenmesi için gerekli bütün kaynaklar belirlenip dokümante edilmelidir. Bunlar veri, algoritma ve geliştirme araçları, yazılım, donanım, ağ, depolama, hesaplama altyapısı ve yetkin insan kaynağını kapsar.

B.5 YZ sistemlerinin etkilerinin değerlendirilmesi

- **B.5.1 Amaç**
- **B.5.2 YZ sistemi etki değerlendirmesi süreci**
- **B.5.3 YZ sistemi etki değerlendirmelerinin dokümantasyonu**
- **B.5.4 YZ sisteminin bireyler veya birey grupları üzerindeki etkilerinin değerlendirilmesi**
- **B.5.5 YZ sistemlerinin toplumsal etkilerinin değerlendirilmesi**

YZ sisteminin bireyler, belirli gruplar ve toplum üzerindeki olumlu ve olumsuz sonuçları değerlendirilir. Etki değerlendirmesi; kullanım amacı, teknoloji karmaşıklığı, otomasyon düzeyi, kullanılan veriler, insan hakları, sağlık, güvenlik, hakkaniyet ve toplumsal etkileri kapsamalıdır. Sonuçlar kaydedilmeli ve değişiklik olduğunda güncellenmelidir.

B.6 YZ sistemi yaşam döngüsü

B.6.1 YZ sistemi geliştirilmesine ilişkin yönetim rehberliği

- **B.6.1.1 Amaç**
- **B.6.1.2 YZ sisteminin sorumlu geliştirilmesine ilişkin amaçlar**
- **B.6.1.3 YZ sistemlerinin sorumlu tasarım ve geliştirme süreçleri**

B.6.2 YZ sistemi yaşam döngüsü

- **B.6.2.1 Amaç**
- **B.6.2.2 YZ sistemi gereksinimleri ve özellikleri**
- **B.6.2.3 YZ sistemi tasarım ve geliştirmesinin dokümantasyonu**
- **B.6.2.4 YZ sisteminin doğrulanması ve geçerli kılınması**
- **B.6.2.5 YZ sisteminin kullanıma alınması**
- **B.6.2.6 YZ sisteminin işletilmesi ve izlenmesi**
- **B.6.2.7 YZ sistemi teknik dokümantasyonu**
- **B.6.2.8 YZ sisteminin olay günlüklerini kaydetmesi**

YZ sisteminin gereksinimlerinin belirlenmesinden tasarım, geliştirme, doğrulama, geçerli kılma ve kullanıma almaya; canlı kullanım, izleme, teknik dokümantasyon ve olay kayıtlarına kadar bütün yaşam döngüsünü kapsar. Sorumlu geliştirme amaçları her aşamaya yerleştirilmeli ve kararlar izlenebilir olmalıdır.

B.7 YZ sistemleri için veri

B.7.1 Amaç
B.7.2 YZ sisteminin geliştirilmesi ve iyileştirilmesi için veri
B.7.3 Verinin edinilmesi
B.7.4 YZ sistemleri için veri kalitesi
B.7.5 Veri kökeni
B.7.6 Verinin hazırlanması

Geliştirme, eğitim, doğrulama, test ve kullanım verilerinin uygunluğu yönetilir. Veri ediniminin hukuka uygunluğu, veri kalitesi, temsil gücü, kökeni, etiketlenmesi, hazırlanması ve dönüşümleri dokümante edilmelidir.

B.8 YZ sistemleriyle ilgili taraflara sunulan bilgiler

B.8.1 Amaç
B.8.2 Sistem dokümantasyonu ve kullanıcılara sunulan bilgiler
B.8.3 Dış bildirim
B.8.4 Olayların iletişimi
B.8.5 İlgili taraflara sunulan bilgiler

Kullanıcıların bir YZ sistemiyle etkileşimde olduklarını, sistemin amacını, kullanım sınırlarını, performansını, insan gözetimi gereksinimini ve olası yarar veya zararlarını anlayabilmeleri sağlanmalıdır. Dışarıdan olay bildirimi alınmalı ve olayların kullanıcılar, yetkili kurumlar ve diğer ilgili taraflarla iletişimi planlanmalıdır.

B.9 YZ sistemlerinin kullanılması

B.9.1 Amaç
B.9.2 YZ sistemlerinin sorumlu kullanımına ilişkin süreçler
B.9.3 YZ sisteminin sorumlu kullanımına ilişkin amaçlar
B.9.4 YZ sisteminin amaçlanan kullanımı

Kuruluş, YZ sistemlerini kendi politikaları ve sorumlu kullanım amaçları doğrultusunda kullanmalıdır. Hakkaniyet, hesap verebilirlik, şeffaflık, açıklanabilirlik, güvenilirlik, güvenlik, sağlamlık, mahremiyet ve erişilebilirlik amaçları dikkate alınır. Sistem, amaçlanan kullanım ve üretici dokümantasyonu dışında kullanılmamalıdır.

B.10 Üçüncü taraf ve müşteri ilişkileri

B.10.1 Amaç
B.10.2 Sorumlulukların dağıtılması
B.10.3 Tedarikçiler
B.10.4 Müşteriler

YZ yaşam döngüsünde kuruluş, tedarikçi, geliştirici, veri sağlayıcı, müşteri ve diğer üçüncü taraflar arasındaki sorumluluklar açıkça dağıtılmalıdır. Tedarikçilerin kuruluşun sorumlu YZ yaklaşımına uygunluğu değerlendirilmeli; müşterilere sistemin kullanım sınırları ve gerekli bilgiler sunulmalıdır.

Ek C. Potansiyel YZ ile ilişkili kurumsal hedefler ve risk kaynakları (Bilgilendirici)

“Annex C (informative) — Potential AI-related organizational objectives and risk sources”

Yapay zekâ hedefleri ve olası risk kaynakları hakkında açıklayıcı bilgi verir.

C.1 Genel

Kuruluşun YZ risklerini yönetirken dikkate alabileceği amaç ve risk kaynaklarından örnekler verir. Liste kapsamlı veya her kuruluş için zorunlu değildir. Kuruluş kendi bağlamına uygun olanları seçmelidir.

C.2 Amaçlar

C.2.1 Hesap verebilirlik
C.2.2 YZ uzmanlığı
C.2.3 Eğitim, doğrulama ve test verilerinin bulunabilirliği ve kalitesi
C.2.4 Çevresel etki
C.2.5 Hakkaniyet
C.2.6 Sürdürülebilir bakım yapılabilirlik
C.2.7 Mahremiyet
C.2.8 Sağlamlık
C.2.9 Güvenlik
C.2.10 Bilgi güvenliği
C.2.11 Şeffaflık ve açıklanabilirlik

Bu maddeler, kuruluşun YZ sistemleri için belirleyebileceği güvenilirlik ve sorumlu kullanım amaçlarını gösterir. Amaçlar; görevlerin hesap verebilir biçimde dağıtılması, yeterli uzmanlık, uygun veri, hakkaniyet, mahremiyet, güvenli çalışma, saldırılara dayanıklılık, sistemin bakımının sürdürülebilmesi ve sonuçların açıklanabilmesini kapsar.

Buradaki iki İngilizce kavramın ayrılması önemlidir:

- **Safety:** İnsan yaşamının, sağlığın, malın veya çevrenin tehlikeye girmemesi
- **Security:** Yetkisiz erişim, saldırı, manipülasyon ve bilgi güvenliği risklerine karşı korunma

C.3 Risk kaynakları

- **C.3.1 Ortamın karmaşıklığı**
- **C.3.2 Şeffaflık ve açıklanabilirlik eksikliği**
- **C.3.3 Otomasyon düzeyi**
- **C.3.4 Makine öğrenmesiyle ilişkili risk kaynakları**
- **C.3.5 Sistem donanımı sorunları**
- **C.3.6 Sistem yaşam döngüsü sorunları**
- **C.3.7 Teknolojinin hazır olma düzeyi**

Risk kaynakları; sistemin çalıştığı ortamın çeşitliliği, kararların açıklanamaması, yüksek otomasyon, veri ve makine öğrenmesi sorunları, donanım arızaları, tasarım veya kullanıma alma hataları, yetersiz bakım, performans sapması ve teknolojinin yeterince olgunlaşmamış olmasıdır.

Ek C, risk listesinin kendisi değildir; **kuruluşun YZ risk envanterini hazırlarken kullanabileceği bir başlangıç kaynağıdır.**

Ek D. YZ Yönetim Sisteminin Farklı Alan veya Sektörlerde Kullanılması ve Bütünlerştirilmesi (Bilgilendirici)

Annex D (informative) — Use of the AI management system across domains or sectors

Standardın farklı sektörlerde kullanılması ve diğer yönetim sistemi standartlarıyla bütünleştirilmesini açıklar.

D.1 Genel

YZ yönetim sisteminin YZ geliştiren, sağlayan veya kullanan bütün kuruluşlara uygulanabileceğini açıklar. Sağlık, savunma, ulaşım, finans, istihdam ve enerji örnek sektörler olarak verilir.

YZ sistemi tek başına algoritmadan oluşmaz; veri, yazılım, donanım, bilgi sistemi, kullanıcılar ve kurumsal süreçlerle birlikte çalışır. Bu nedenle güvenlik, mahremiyet, kalite ve çevresel etkiler YZ'den ayrı yönetilmemeli; kuruluşun mevcut yönetim sistemleriyle bütünleştirilmelidir.

D.2 YZ yönetim sisteminin diğer yönetim sistemi standartlarıyla bütünleştirilmesi

Metinde ele alınan başlıca standartlar

- **ISO/IEC 27001: Bilgi güvenliği yönetim sistemi**

ISO/IEC 27701: Mahremiyet bilgi yönetimi
ISO 9001: Kalite yönetim sistemi
ISO 22000: Gıda güvenliği yönetim sistemi
ISO 13485: Tıbbi cihaz kalite yönetim sistemi
IEC 62304: Tıbbi cihaz yazılımı yaşam döngüsü süreçleri

ISO/IEC 42001'in diğer yönetim sistemi standartlarıyla birlikte kurulabileceğini açıklar. Ortak yüksek düzeyli yapı, politika, risk yönetimi, dokümantasyon, iç tetkik, yönetimin gözden geçirmesi ve iyileştirme süreçlerinin bütünleştirilmesini kolaylaştırır.

Tıbbi laboratuvar açısından Ek D'nin temel mesajı şöyledir:

ISO/IEC 42001, laboratuvarın mevcut kalite yönetim sisteminden bağımsız yürütülmemeli; ISO 15189'a dayalı süreç, risk, bilgi, kaynak, değerlendirme ve iyileştirme yapısıyla bütünleştirilmelidir.

ISO 15189, Ek D'de örnek olarak açıkça sayılmasa da aynı bütünleştirme yaklaşımı tıbbi laboratuvar yönetim sistemine uygulanabilir.

Kuruluşun hazırlaması gereken temel yapılar

ISO/IEC 42001'e göre kuruluşta en azından şu yapıların bulunması beklenir:

- YZ yönetim sistemi kapsamı
- YZ politikası
- YZ sistemleri envanteri
- Görev, yetki ve sorumluluklar
- YZ risk değerlendirme yöntemi ve risk envanteri
- YZ risk işleme planı
- Uygulanabilirlik Bildirgesi
- YZ sistemi etki değerlendirmeleri
- YZ hedefleri ve göstergeleri
- Veri ve yaşam döngüsü yönetimi
- İnsan gözetimi
- Tedarikçi ve üçüncü taraf kontrolleri
- Olay ve uygunsuzluk kayıtları
- Değişiklik yönetimi
- İç tetkik
- Yönetimin gözden geçirmesi
- Düzeltici faaliyet ve sürekli iyileştirme

Tıbbi laboratuvara uygulanması

Tıbbi laboratuvarda ISO/IEC 42001, ISO 15189'dan bağımsız ikinci bir dokümantasyon sistemi olarak kurulmak zorunda değildir. Ortak yönetim süreçleri bütünleştirilebilir.

- ISO 15189 laboratuvarın kalite ve yeterlilik sistemini,
- ISO/IEC 42001 kuruluş düzeyinde yapay zekâ yönetişimini,
- ISO 24051-1 ise belirli YZ sisteminin laboratuvarda değerlendirilmesi, kullanıma alınması ve izlenmesini

düzenler.

Özetlenirse;

ISO/IEC 42001'in temel yaklaşımı şöyledir:

Kuruluşun yapay zekâ sistemlerini envantere al; politika, görev ve sorumlulukları belirle; riskleri ve bireyler ile toplum üzerindeki etkileri değerlendir; uygun kontrolleri seç; yapay zekâ yaşam döngüsünü, verileri ve üçüncü tarafları yönet; performansı iç tetkik ve yönetimin gözden geçirmesiyle değerlendir; uygunsuzlukları gidererek sistemi sürekli iyileştir.

Yapay zekâ kullanımına ilişkin açıklama: Bu çalışmanın yapılandırılmasında ve ilk taslağının hazırlanmasında OpenAI ChatGPT'den yararlanılmıştır. İçerik, özgün kaynaklar esas alınarak yazar tarafından doğrulanmış ve düzeltilmiş; çalışmanın son biçimi yazar tarafından verilmiştir.

Yazar hakkında

Prof. Dr. Diler Aslan, tıbbi biyokimya, tıbbi laboratuvar yönetimi, laboratuvar verilerinin yönetimi ve kalite sistemleri alanlarında uzun yıllar akademik ve uygulamalı çalışmalar yürütmüş; çeşitli kurumsal yöneticilik görevlerinde bulunmuştur. FORTRAN II Programlama Dili (1972), ANKUZEM E-Eğitimci (2013), UKAS ISO/IEC 42001 Yapay Zekâ Yönetim Sistemleri Farkındalık (2025) ve ADLM Tıbbi Laboratuvarlarda Veri Bilimi (2026) eğitimlerini tamamlamıştır. Dijital sağlık, veri kalitesi, yapay zekâ yönetişimi ve tıbbi laboratuvarlarda kalite yönetimi alanlarında eğitim ve danışmanlık çalışmalarını sürdürmektedir. ORCID: 0000-0003-4907-9445