# Data Governance and Ethics (MSCAI1)- Ders Özeti

* **Eğitmen:** Arundev Vamadevan
* **Ders İçeriği:**
  + **Hafta 1-3:** Veri Yönetişimi ve Yönetimi
  + **Hafta 4-5:** Gizlilik ve Veri Koruma
  + **Hafta 6, 8-9:** Veriye İlişkin Etik Sorunlar
  + **Hafta 10-12:** Algoritmik Sistemlerin Adalet, Hesap Verebilirlik ve Şeffaflığı

**Veri Yönetişimi (Data Governance)**

* **Tanım:** Bir organizasyon içindeki veri varlıklarının resmi olarak yönetilmesini sağlamak için kullanılan uygulamalar ve süreçler bütünüdür.
* **Önemi:** Veri kullanılabilirliği, güvenliği ve bütünlüğünü yönetmeye yardımcı olur.
* **Bileşenler:**
  + **Kurallar:** Verinin ne kadar süre saklanacağı, nerede depolanacağı ve kimlerin erişebileceği gibi konuları belirler.
  + **Süreçler:** Veri taleplerinin nasıl yapılacağını ve verinin güvenliğini sağlama yöntemlerini tanımlar.
  + **Hesap Verebilirlik:** Veriyle ilgili sorumlulukları ve karar alma süreçlerini belirler.

**Veri Yönetişiminin Faydaları**

* Yasal düzenlemelere ve veri gizliliği yasalarına uyumu sağlar.
* Karar verme süreçleri için güvenilir ve kaliteli veri sağlar.
* Veri ihlalleri, uyumsuzluk, itibar kaybı ve yanlış analiz sonuçları gibi riskleri önler.

**ABD Veri Gizliliği Düzenlemeleri**

* **HIPAA (1997):** Hasta bilgilerini korur.
* **CCPA (2018):** Kaliforniya sakinlerine kişisel verilerinin kullanımı ve yönetimi üzerinde daha fazla kontrol sağlar.

**Genel Veri Koruma Yönetmeliği (GDPR)**

* **Kapsam:** AB vatandaşlarının verilerini toplayan herhangi bir şirketi kapsar.
* **Ana Unsurlar:**
  + Kişisel verilerin işlenmesi konusunda bireylerin haklarını artırır.
  + Verilerin anonimleştirilmesini ve ihlallerin bildirilmesini gerektirir.
  + Ülkeler arası veri transferleri için belirli standartları belirler.
  + Bazı şirketlerin bir Veri Koruma Görevlisi bulundurmasını zorunlu kılar.

**Veri Sınıflandırması ve Saklama**

* **Veri Sınıflandırması:** Veriyi gizlilik düzeyine göre gruplandırır ve nasıl işleneceğini belirler.
* **Saklama Politikaları:** Verinin ne kadar süreyle saklanacağını ve ne zaman imha edileceğini belirler.

**Kötü Veri Yönetişiminin Sonuçları**

* **Örnek:** Cambridge Analytica skandalı.
* **Olası Riskler:**
  + Veri ihlalleri
  + Uyumsuzluk
  + İtibar kaybı
  + Mali cezalar
* **GDPR Cezaları:** Amazon (886 milyon $) ve WhatsApp (267 milyon $) gibi büyük cezalar.

**Veri Yönetişiminin Başarısız Olma Nedenleri**

* Net bir tanımın olmaması
* Merkezi bir karar alma mekanizmasının eksikliği
* Veri yönetişiminin iş meselesi değil, IT sorunu olarak görülmesi
* Başlangıçta belirlenen uygulamanın takip edilmemesi
* Yatırım getirisinin (ROI) net olmaması

**Veri Yönetişiminin Beş Temel Ayağı**

1. **Sahiplik ve Hesap Verebilirlik:** Veri ile ilgili net roller ve sorumluluklar.
2. **Veri Kalitesi:** Verinin doğruluğu ve güvenilirliğinin sağlanması.
3. **Veri Koruma ve Güvenliği:** Veriyi korumak için güvenlik önlemlerinin alınması.
4. **Veri Kullanımı ve Erişilebilirlik:** Verinin raporlama ve analiz için kolayca bulunabilir ve erişilebilir olması.
5. **Veri Yönetimi:** Veri yönetişimi politikalarını destekleyen teknolojilerin kullanımı.

**Veri Yönetişimi vs. Veri Yönetimi**

* **Veri Yönetimi:** Günlük veri işlemleri (depolama, işleme).
* **Veri Yönetişimi:** Verinin nasıl yönetileceğine dair kuralların belirlenmesi.

**DAMA-DMBOK Veri Yönetimi Çerçevesi**

* Verinin yaşam döngüsü boyunca etkili bir şekilde yönetilmesi için en iyi uygulamaları, standartları ve süreçleri içeren kapsamlı bir rehber.
* Verinin iş hedeflerine ulaşmada değerli bir varlık olmasını sağlar.

# Study Notes for Data Governance Frameworks and Implementation

## 1. Introduction to Data Governance (Veri Yönetimi)

**Tanım**: Veri yönetimi, bir organizasyonda verilerin kullanılabilirliği, bütünlüğü, güvenliği ve kullanılabilirliğini sağlayan yönetim çerçevesine denir. Veri yönetimi, politikalar, roller, standartlar ve ölçütler içeren süreçleri ve sorumlulukları net bir şekilde belirler ve verilerin etkili bir şekilde kullanılmasını ve düzenlemelere uygunluğunu sağlar.

🚩 **Ana Bileşenler**:

* **Data Ownership & Stewardship (Veri Sahipliği ve Yönetimi)**: Verilerin yönetiminden sorumlu kişileri belirlemek.
* **Data Quality Management (Veri Kalite Yönetimi)**: Verilerin doğruluğunu, tutarlılığını ve bütünlüğünü sağlamak.
* **Data Security & Privacy (Veri Güvenliği ve Gizliliği)**: Hassas bilgileri korumak ve GDPR gibi düzenlemelere uyumu sağlamak.
* **Data Lifecycle Management (Veri Yaşam Döngüsü Yönetimi)**: Verinin toplanması, saklanması, kullanılması, arşivlenmesi ve imha edilmesini yönetmek.
* **Compliance & Regulatory Requirements (Uyum ve Yasal Gereklilikler)**: Organizasyonun veri uygulamalarının sektör standartlarına ve yasal yükümlülüklere uygun olmasını sağlamak.
* **Data Cataloging & Classification (Veri Kataloğu ve Sınıflandırması)**: Verilerin kolayca bulunması ve yetkili kullanıcılar tarafından kullanılması için organize edilmesi ve sınıflandırılması.

## 2. Data Governance Framework (Veri Yönetim Çerçevesi)

Verilerin yaşam döngüsü boyunca etkili bir şekilde yönetilmesini sağlamak için bir organizasyonun izlediği yapılandırılmış yönergeler ve uygulamalar setidir.

🚩 **Ana Bileşenler**:

* **Data Governance Policies and Standards (Veri Yönetimi Politikaları ve Standartları)**: Verilerin nasıl ele alınacağına dair yönergeler.
* **Data Stewardship and Ownership (Veri Sahipliği ve Yöneticiliği)**: Veri yönetimi için net rollerin belirlenmesi.
* **Data Quality Management (Veri Kalitesi Yönetimi)**: Verilerin bütünlüğünü korumak.
* **Data Privacy and Security (Veri Gizliliği ve Güvenliği)**: GDPR ve HIPAA gibi gizlilik yasalarına uygun olarak verileri korumak.
* **Metadata Management (Veri Hakkında Veri Yönetimi)**: Verinin bağlamını ve kullanımını geliştirmek için veri hakkında veri yönetimi.
* **Compliance (Uyum)**: Yasal standartlarla uyumun sağlanması.
* **Data Architecture and Infrastructure (Veri Mimarisi ve Altyapısı)**: Veri yönetimi için teknik altyapının oluşturulması.
* **Data Cataloging (Veri Kataloglama)**: Verilerin daha iyi erişim için belgelenmesi ve sınıflandırılması.
* **Roles and Responsibilities (Roller ve Sorumluluklar)**: Chief Data Officer (CDO) gibi rollerin tanımlanması.

## 3. Popular Data Governance Frameworks (Popüler Veri Yönetimi Çerçeveleri)

🚩 **Örnekler**:

* **DAMA-DMBOK**: Veri yönetimi için kapsamlı yönergeler.
* **COBIT**: Veri bileşenlerini içeren bir BT yönetim çerçevesi.
* **ISO/IEC 38500**: Veri yönetimini de içeren BT yönetimi için uluslararası bir standart.
* **CMMI**: Veri yönetimi olgunluk seviyelerini geliştirmeye yönelik bir çerçeve.

## 4. Implementation Steps for a Data Governance Framework (Veri Yönetimi Çerçevesi Uygulama Adımları)

**1. Planning and Strategy Development (Planlama ve Strateji Geliştirme)**

* Mevcut veri yönetimi uygulamalarını değerlendir ve yönetim hedeflerini belirle.

**2. Assigning Roles and Responsibilities (Roller ve Sorumlulukların Atanması)**

* CDO gibi kilit paydaşlardan oluşan bir Veri Yönetimi Komitesi oluştur.
* **Data Owners (Veri Sahipleri)**, **Data Stewards (Veri Yöneticileri)** ve **Data Custodians (Veri Koruyucuları)** gibi rollerin tanımlanması.

**3. Data Management and Handling (Veri Yönetimi ve İşleme)**

* **Veri Toplama ve Saklama (Data Collection and Storage)**: Tutarlılık ve güvenlik için standartlaştırılmış süreçler uygulayın.
* **Veri İşleme ve Entegrasyonu (Data Processing and Integration)**: Sistemler arasında veri tutarlılığını sağlayın.

## 4. Policy Creation and Enforcement (Politika Oluşturma ve Uygulama)

* Veri erişimi, güvenliği ve şifreleme gibi konularda politikalar oluştur.
* Düzenli denetimlerle bu politikalara uyumu sağla.

## 5. Monitoring and Evaluation (İzleme ve Değerlendirme)

* Veri kalitesini ve yönetim faaliyetlerini izlemek için sürekli izleme araçlarını kullan.
* Verilen geri bildirimlerle veri yönetimi süreçlerini düzenli olarak değerlendir.

## 6. Continuous Improvement (Sürekli İyileştirme)

* İş hedefleri ve teknolojik değişikliklerle uyumlu olarak veri yönetim çerçevesini sürekli güncelle.
* Eğitim programları ile tüm paydaşların rollerini anlamalarını sağla.

## Study Notes for Roles and Responsibilities in Data Governance

#### 1. Key Roles in Data Governance (Veri Yönetimindeki Kilit Roller)

🚩 **Chief Data Officer (CDO)**  
**Türkçe**: Baş Veri Sorumlusu  
**Açıklama**: CDO, veri yönetiminin lideri olarak görev yapar ve veri yönetimi inisiyatifini tüm departmanlarda yönlendirir.

🚩 **Data Governance Council / Steering Committee**  
**Türkçe**: Veri Yönetim Konseyi / Yürütme Komitesi  
**Açıklama**: Bu konsey, veri yönetiminin tüm iş birimlerinin ihtiyaçlarıyla uyumlu olmasını sağlamak amacıyla farklı departmanlardan kıdemli paydaşlardan oluşur.

🚩 **Data Owner**  
**Türkçe**: Veri Sahibi  
**Açıklama**: Veri sahipleri, kendi sorumluluk alanlarındaki (örneğin müşteri verileri, finansal veriler) verilerin korunmasından ve doğru kullanımından sorumludur.

🚩 **Data Steward**  
**Türkçe**: Veri Yöneticisi  
**Açıklama**: Veri yöneticileri, verilerin iyi yönetildiğini ve veri yönetimi politikalarına uyduğunu garanti eder. Veri yönetiminin operasyonel yüzü olarak görev yaparlar.

🚩 **Data Custodian**  
**Türkçe**: Veri Koruyucusu  
**Açıklama**: Veri koruyucuları, verilerin doğru bir şekilde saklanmasını, güvenliğini ve ihtiyaç duyulduğunda erişilebilir olmasını sağlayan teknik sorumlulardır.

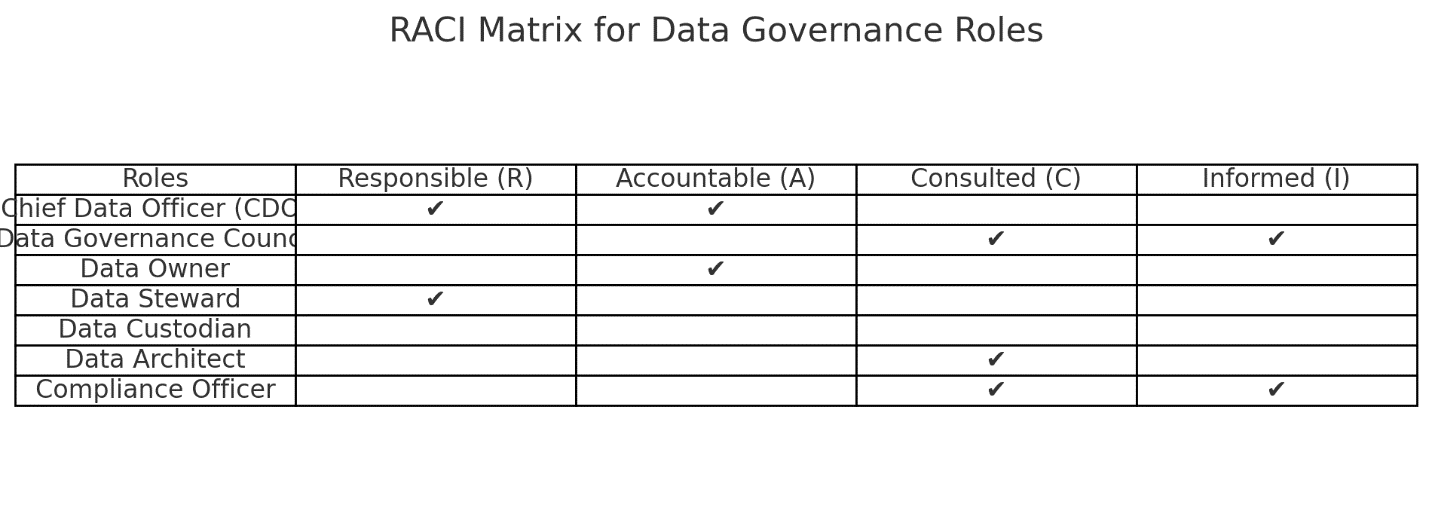
🚩 **Data Architect**  
**Türkçe**: Veri Mimarı  
**Açıklama**: Veri mimarları, teknik veri altyapısının iş ihtiyaçlarını destekleyecek şekilde organize edilmesini ve yönetim hedefleriyle uyumlu olmasını sağlar.

🚩 **Compliance Officer / Legal Team**  
**Türkçe**: Uyum Görevlisi / Hukuk Ekibi  
**Açıklama**: Uyum görevlileri, organizasyonun veri uygulamalarının yasal ve düzenleyici yükümlülüklere uygun olmasını sağlar ve cezai yaptırımların ve itibar kaybının önlenmesine yardımcı olur.

#### 2. Data Governance Roles and Responsibilities Matrix (Veri Yönetimi Roller ve Sorumluluk Matrisi)

**RACI Matrisi**:

* **R: Responsible (Sorumlu)** – Görevleri yerine getiren kişi (örneğin, veri kalitesini yöneten veri yöneticisi).
* **A: Accountable (Hesap Veren)** – Görevden nihai olarak sorumlu kişi (örneğin, değişiklikleri onaylayan veri sahibi).
* **C: Consulted (Danışılan)** – Fikir alınan kişiler (örneğin, sistem değişikliklerinde veri mimarı).
* **I: Informed (Bilgilendirilen)** – Süreç hakkında bilgilendirilmesi gerekenler (örneğin, CDO, uyum ekibi).



# Study Notes for Policies and Procedures in Data Governance

## 1. Data Governance Policies (Veri Yönetimi Politikaları)

**Tanım**:  
Veri yönetimi politikaları, organizasyon genelinde verilerin nasıl yönetileceğini, erişileceğini ve kullanılacağını belirleyen yüksek seviyede kurallar ve yönergelerdir. Bu politikalar, verilerin iş hedefleri ve düzenleyici gereksinimlerle uyumlu bir şekilde güvenli ve tutarlı olarak ele alınmasını sağlar.

🚩 **Örnekler**:

* **Data Access Policy (Veri Erişim Politikası)**: Finans departmanındaki çalışanlar finansal kayıtlara erişebilirken, diğer departmanlar sadece toplu raporlara erişebilir. Rol tabanlı erişim kontrolü uygulanır.
* **Data Retention Policy (Veri Saklama Politikası)**: Müşteri verileri yedi yıl boyunca saklanmalı ve ardından yerel veri koruma yasalarına uygun olarak güvenli bir şekilde silinmelidir.

## 2. Data Governance Processes (Veri Yönetimi Süreçleri)

**Tanım**:  
Veri yönetimi süreçleri, veri yönetimi politikalarını hayata geçiren operasyonel iş akışlarıdır. Verilerin yaşam döngüsü boyunca nasıl ele alınacağını, yani oluşturulmasından imhasına kadar tüm adımları tanımlar.

🚩 **Örnekler**:

* **Data Collection Process (Veri Toplama Süreci)**: Müşteri verileri online formlar aracılığıyla toplanır, bir CRM veritabanına karşı doğrulanır ve yalnızca gerekli alanlar (isim, e-posta vb.) doldurulduğunda sisteme girilir.
* **Data Quality Process (Veri Kalitesi Süreci)**: Haftalık olarak çalışan otomatik komut dosyaları, veritabanlarındaki eksik değerleri ve tekrar eden verileri temizleyerek veri tutarsızlıklarını belirler.

## 3. Data Governance Procedures (Veri Yönetimi Prosedürleri)

**Tanım**:  
Veri yönetimi prosedürleri, veri yönetimi süreçlerini günlük operasyonlarda nasıl uygulayacaklarını adım adım açıklayan detaylı talimatlardır. Bu prosedürler, çalışanların verileri belirlenen politikalar ve süreçlere uygun şekilde nasıl ele alacaklarını anlamalarına yardımcı olur.

🚩 **Örnekler**:

* **Procedure for Data Access Request (Veri Erişim Talebi Prosedürü)**:
  1. Çalışan, veri yönetimi portalı üzerinden bir veri erişim talebi gönderir.
  2. Veri yöneticisi (Data Steward) talebi inceleyip çalışanın rolünü ve erişim haklarını doğrular.
  3. Onaydan sonra, belirlenen izinlerle erişim sağlanır.
  4. Denetim amaçlı olarak sistemde bir kayıt girişi yapılır.

## 4. How These Components Work Together (Bu Bileşenlerin Nasıl Birlikte Çalıştığı)

**Örnek Durum**:  
Bir sağlık kuruluşunun hasta kayıtları için veri yönetimi uyguladığını düşünelim.

1. **Politikalar (Policies)**, genel kuralları ve ilkeleri sağlar.
   * **Data Privacy Policy (Veri Gizliliği Politikası)**: Hasta verilerine yalnızca yetkili sağlık personeli erişebilir ve bu veriler HIPAA düzenlemelerine uygun olmalıdır.
   * **Data Retention Policy (Veri Saklama Politikası)**: Hasta kayıtları on yıl boyunca saklanmalı ve ardından güvenli bir şekilde silinmelidir.
2. **Süreçler (Processes)**, bu politikaların nasıl uygulanacağını tanımlar.
   * **Patient Data Collection Process (Hasta Verileri Toplama Süreci)**: Veriler, hasta kabul işlemleri sırasında toplanır, mevcut kayıtlarla doğrulanır ve Elektronik Sağlık Kaydı (EHR) sisteminde saklanır.
   * **Data Access Process (Veri Erişim Süreci)**: Doktorlar hasta kayıtlarına güvenli bir platform üzerinden erişim talebinde bulunur ve talep veri yöneticisi tarafından incelenir.
3. **Prosedürler (Procedures)**, spesifik adımları sağlar.
   * **Patient Data Entry Procedure (Hasta Verisi Giriş Prosedürü)**: Personel, hasta bilgilerini EHR sistemine girerken önceden belirlenmiş adımları takip eder, mükerrer kayıtları kontrol eder ve tüm gerekli alanların doldurulduğundan emin olur.
   * **Data Breach Incident Procedure (Veri İhlali Olayı Prosedürü)**: Bir veri ihlali meydana gelirse, olay veri yönetim ekibine bildirilir ve olayın ele alınması, araştırılması ve çözülmesi için belgelenmiş bir prosedür izlenir.

**Özet**:

* **Politikalar (Policies)** kuralları sağlar.
* **Süreçler (Processes)** iş akışını açıklar.
* **Prosedürler (Procedures)** günlük görevler için detaylı talimatlar sunar.

Bu bileşenlerin uyumlu çalışması, organizasyonun güvenilir, güvenli ve iş hedefleriyle uyumlu bir veri yönetimi çerçevesi oluşturmasını sağlar.

# Study Notes for Data Quality and Provenance

## 1. Types of Enterprise Data (Kurumsal Veri Türleri)

🚩 **Transactional Data (İşlem Verisi)**:  
Günlük iş operasyonlarından üretilen veriler, örneğin satış siparişleri, ödemeler veya müşteri etkileşimleri. Gerçek zamanlı faaliyetleri yansıtır ve genellikle kısa vadeli karar verme için kullanılır.

🚩 **Analytical Data (Analitik Veri)**:  
Geçmiş performanstan elde edilen içgörüleri analiz etmek ve raporlamak için kullanılan veriler. İş zekası araçlarında, stratejik kararlar için rehberlik eder.

🚩 **Master Data (Ana Veri)**:  
Müşteriler, ürünler veya çalışanlar gibi temel iş varlıklarını tanımlayan veriler. Farklı sistemler arasında tutarlılığı sağlar ve doğru bilgi kaynağı olarak kullanılır.

## 2. The 5 Stages of Data Life Cycle Management (Veri Yaşam Döngüsü Yönetiminin 5 Aşaması)

🚩 **1. Data Creation (Veri Oluşturma)**:  
Verinin oluşturulması veya yakalanması. Veriler, veri edinimi, manuel giriş veya cihazlar aracılığıyla yakalanabilir.

🚩 **2. Storage (Depolama)**:  
Veri oluşturulduktan sonra uygun güvenlik önlemleriyle korunmalı ve saklanmalıdır. Güçlü bir yedekleme ve kurtarma süreci uygulanmalıdır.

🚩 **3. Usage (Kullanım)**:  
Veri iş faaliyetlerini desteklemek için kullanılır, işlenir ve saklanır. Tüm kritik veriler için bir denetim kaydı tutulmalıdır.

🚩 **4. Archival (Arşivleme)**:  
Veriler aktif üretim ortamlarından çıkarılır ve gerekirse kullanılmak üzere arşiv ortamına kopyalanır.

🚩 **5. Destruction (İmha)**:  
Veriler, düzenleyici saklama süresini aşarsa ve artık gerekli değilse güvenli bir şekilde imha edilir. Tüm veri kopyalarının yok edildiğinden emin olunmalıdır.

## 3. Data Quality (Veri Kalitesi)

Veri kalitesi, verinin doğru, anomali içermeyen ve amacına uygun olmasını sağlar. Düşük veri kalitesi, yanlış içgörülere ve iş operasyonlarında olumsuz etkilere neden olabilir.

🚩 **Önemi**:

* **Better Decision-Making (Daha İyi Karar Verme)**: Yüksek kaliteli veriler, doğru içgörüler sağlar ve iş kararlarını destekler.
* **Operational Efficiency (Operasyonel Verimlilik)**: Hataların azalmasıyla süreçler daha akıcı hale gelir.
* **Regulatory Compliance (Düzenleyici Uyum)**: Hatalı veya eksik veri, düzenleyici gereksinimlere uymama riskini doğurabilir.
* **Improved Analytics (Gelişmiş Analitik)**: Temiz, doğru veri, güvenilir analitik modeller sağlar.

🚩 **Veri Kalitesinin Boyutları**:

* **Accuracy (Doğruluk)**: Verilerin gerçek dünyadaki değerleri doğru bir şekilde yansıtması.
* **Completeness (Tamlık)**: Gerekli tüm verilerin mevcut olması.
* **Consistency (Tutarlılık)**: Verilerin tüm sistemlerde uyumlu olması.
* **Timeliness (Zamanında Olma)**: Verilerin güncel olması.
* **Validity (Geçerlilik)**: Verilerin belirlenmiş formatlara ve kurallara uygun olması.
* **Uniqueness (Benzersizlik)**: Tekrar eden kayıtların olmaması.

## 4. Data Provenance (Veri Geçmişi)

🚩 **Tanım**:  
Verilerin kökeni ve tarihçesi hakkında ayrıntılı bilgi sağlar. Verinin nereden geldiğini, nasıl işlendiğini, dönüştürüldüğünü ve organizasyonda nasıl kullanıldığını kaydeder.

🚩 **Ana Bileşenler**:

* **Source of Data (Veri Kaynağı)**: Verilerin nereden geldiğine dair bilgi sağlar (örneğin, web formları, CRM sistemleri).
* **Transformation Process (Dönüşüm Süreci)**: Verilerin nasıl işlendiği veya dönüştürüldüğünü açıklar.
* **Tracking Changes (Değişikliklerin Takibi)**: Verilerde yapılan değişikliklerin kim tarafından ve ne zaman yapıldığını kaydeder.
* **Data Movement (Veri Hareketi)**: Verilerin organizasyon içinde hangi sistemlerden geçtiğini izler.
* **Ownership & Permissions (Sahiplik ve İzinler)**: Verilerin kim tarafından sahiplenildiği ve kimlerin erişim yetkisi olduğu bilgilerini içerir.

🚩 **Veri Geçmişinin Önemi**:

* **Traceability (İzlenebilirlik)**: Hataların izlenmesi ve güvenilirliğin sağlanması için tam bir denetim izi sunar.
* **Data Trust (Veri Güvenilirliği)**: Verilerin nasıl işlendiğini anlamak, karar vericilerin veriye güvenmesini sağlar.
* **Error Tracking (Hata Takibi)**: Veriyle ilgili sorunları çözmede yardımcı olur.
* **Compliance (Uyum)**: Düzenleyici gerekliliklere uygunluğu sağlar.
* **Data Governance (Veri Yönetimi)**: Veri yaşam döngüsü boyunca tutarlı ve sorumlu veri yönetimini destekler.

# Study Notes for Data Integrity and Security

## 1. Data Integrity (Veri Bütünlüğü)

**Tanım**:  
Veri bütünlüğü, verilerin yaşam döngüsü boyunca doğruluğunu, tutarlılığını ve güvenilirliğini sağlamak anlamına gelir. Verilerin yaratılmasından silinmesine kadar geçen sürede doğru, eksiksiz ve güvenilir kalmasını sağlar.

🚩 **Veri Bütünlüğünün Önemi**:  
Güçlü veri bütünlüğü uygulamaları, organizasyonların güvenilir kararlar almasını, düzenlemelere uyum sağlamasını ve operasyonel verimliliği korumasını sağlar.

🚩 **Veri Bütünlüğü Türleri**:

* **Physical Integrity (Fiziksel Bütünlük)**: Verilerin fiziksel zararlardan korunmasını sağlar (örneğin, donanım arızası, doğal afetler).
  + **Önlemler**: Yedeklemeler, fiziksel güvenlik, felaket kurtarma planları.
* **Logical Integrity (Mantıksal Bütünlük)**: Verilerin nerede saklandığı veya nasıl işlendiğine bakılmaksızın tutarlı, geçerli ve doğru kalmasını sağlar.
  + **Önlemler**: Veritabanı kısıtlamaları, veri doğrulama, hata denetim mekanizmaları.

🚩 **Mantıksal Bütünlük Alt Türleri**:

* **Entity Integrity (Varlık Bütünlüğü)**: Her veri kaydının benzersiz bir kimliğe sahip olmasını sağlar (örneğin, veritabanlarında birincil anahtarlar).
* **Referential Integrity (Bağlamsal Bütünlük)**: Tablolar arasındaki ilişkilerin tutarlılığını korur (örneğin, geçerli yabancı anahtarlar).
* **Domain Integrity (Alan Bütünlüğü)**: Veri değerlerinin belirli aralıklar veya formatlar içinde olmasını sağlar (örneğin, tarih alanlarına yalnızca geçerli tarihler girilebilir).

## 2. Data Security (Veri Güvenliği)

**Tanım**:  
Veri güvenliği, verilerin yetkisiz erişime veya bozulmaya karşı korunmasını ifade eder ve veri bütünlüğünü sağlamak için gereklidir.

🚩 **Veri Güvenlik Önlemleri**:

* **Policies and Procedures (Politikalar ve Prosedürler)**: Verilerin kullanımı ve güvenliğiyle ilgili net politikalar ve prosedürler.
* **Encryption (Şifreleme)**: Hassas bilgileri korumak için kullanılan bir yöntem.
* **Access Controls (Erişim Kontrolleri)**: Depolanan verilere erişim sınırlamaları.

## 3. Difference Between Data Security and Data Integrity (Veri Güvenliği ve Veri Bütünlüğü Arasındaki Fark)

**Veri Güvenliği**: Verilerin yetkisiz erişime karşı korunması ve bozulmasının engellenmesi anlamına gelir.  
**Veri Bütünlüğü**: Verilerin doğru, tutarlı ve güvenilir olmasını sağlar. Veri güvenliği, veri bütünlüğünü korumak için temel bir gereksinimdir.