KAMU KURUMLARINDA VERİ TABANI YÖNETİMİ DENETİMİ

(AUDITING OF DATABASE MANAGEMENT IN PUBLIC SECTOR)

Tolgahan ÖZDEN* / Hüseyin ÇALIŞ**

ÖZ

İnternet kullanımının 90'lı yıllardan sonra artmasıyla birlikte dünya bilgi çağına girmiş ve her alanda olduğu gibi kamu kurumları da bu çağa ayak uydurmak zorunda kalmışlardır. Bilgiyi oluşturan en temel kavram veridir. Günümüzde kamu kurumları fiziki ortamda sahip oldukları verilerin birçoğunu oluşturdukları bilgi sistemleri vasıtasıyla elektronik ortamda işlemekte ve sunmaktadır. Kamu kurumları verdikleri hizmetlerin güvenilirliğini, şeffaflığını, doğruluğunu ve kaynakların etkin kullanımını bilgi teknolojileri sistemleri kullanarak artırmaktadır. Bu durum vatandaş odaklı hizmet anlayışını geliştirmektedir. Bilgi, verilerin işlenmesiyle oluştuğu için verinin yönetimi önem arz etmektedir. Veri, veri tabanı yönetim sistemleri araçlarıyla yönetilmektedir. Veri tabanı yönetim sistemleri büyük çaplı verileri saklama, değiştirme ve koruma gibi süreçleri kolaylaştırmaktadır. Kritik öneme sahip veri tabanı yönetim sistemlerinin denetimi ise bu sistemin etkin, etkili ve verimli çalışmasına makul güvence vermektedir.

Kamu kurumları bilgi çağına ayak uydururken, veri tabanı yönetimindeki eksikliklerini, yeni teknoloji önerilerini, bilgi güvenliği farkındalığını denetim fonksiyonunu etkin kullanarak geliştirebilirler. Bu çalışmada, veri tabanı yönetim sürecine ilişkin denetim fonksiyonu kamu kurumları özelinde ele alınarak, idari ve teknik alanda belirlenen risk ve bulgu örnekleri için öneriler geliştirilmekte ve bu önerilerin nasıl izlenmesi gerektiği hakkında görüşler sunulmaktadır.

Anahtar Kelimeler: Bilgi, veri, veri tabanı, veri tabanı yönetimi, veri tabanı yönetimi denetimi, iç denetim, bilgi teknolojileri denetimi.

JEL Kodlaması: M15, M42

ABSTRACT

With the increase of internet usage after the 90s, the world entered the information age and public institutions has to keep up with this era as in every other fields. The most basic concept of knowledge is data. Today, public institutions operate and present many of the data they have in physical environment via the information systems. Public institutions increase the reliability, transparency and correctness of their services by using information technology systems. This situation improves citizen-oriented service. Since the information is generated by processing the data, the management of the data is important. Data is managed by database management systems. The database management system simplifies processes such as store, update and protection of large data sets. The control of critically important database management systems, gives a reasonable assurance on effective, efficient and productive operation of this system.

While the public institutions keep up with the information age, they can improve their database management deficiencies, new technology suggestions, and information security awareness effectively by using the audit function. In this study, the audit function of the database management process is discussed in the context of public institutions, recommendations for risk and finding examples determined in the administrative and technical fields are developed and opinions are given on how these recommendations should be monitored.

Keywords: *Information, data, database, database management, database management auditing, internal audit, information technology audit.*

JEL Classification: *M15, M42*

---

*) İç Denetçi, Tapu ve Kadastro Genel Müdürlüğü, İç Denetim Birimi Başkanlığı, Ankara, Orcid:0000-0001-6560-3177, tolgahanozden@gmail.com

**) İç Denetçi, Tapu ve Kadastro Genel Müdürlüğü, İç Denetim Birimi Başkanlığı, Ankara, Orcid:0000-0001-8230-5286, huseyincalis@gmail.com

Yazı Gönderim Tarihi: 21.01.2019, Yazı Kabul Tarihi: 14.04.2019

1. GİRİŞ

Bilgi teknolojileri kullanımı tüm dünyada olduğu gibi ülkemizde de artmaktadır. Hızla artan teknolojik gelişmeler sonucunda bireyler bilgi ve iletişim teknolojilerini daha yaygın bir şekilde kullanmaktadır. Elektronik ortama taşınan kamu hizmetleri sayesinde, kaynaklar etkin ve verimli kullanılmakta, rasyonel duruma getirilen işlemler daha hızlı sunulmaktadır (Sevinç, 2007:22).

Devlet kurumları hızla gelişen bilgi teknolojileri konularında birçok politika üretmiş ve Cumhurbaşkanlığı Yönetim Sistemi ile Cumhurbaşkanına bağlı "Bilim, Teknoloji ve Yenilik Politikaları Kurulu" oluşturularak konunun önemi açıkça vurgulanmıştır. Kamu sektöründe, bilgi teknolojileri yönetim süreci, bilgi işlem birimleri tarafından yürütülmektedir. Bilgi işlem birimleri, kurumlarda farklı teşkilatlanma yapıları gösterse de en genel anlamda yazılım geliştirme, veri tabanı yönetimi, bilgi güvenliği ve sistem yönetimi olarak 4 temel konu üzerine kurulmuştur. Üst düzey bir bilgi teknolojileri modeli geliştirmiş olmak, kurumsal bilgi yönetiminin organizasyonda sağlıklı çalıştığını garanti etmez. Kurumsal bilgi yönetimi modelinin tasarlanması ilk adımdır, bunu organizasyona uygulamak bir sonraki zorlu adımdır (De Haes ve Van Grembergen, 2006:2). Tüm bu modelleme ve teşkilatlanma, verinin üretilmesi, saklanması, güvende tutulması ve istenildiğinde ulaşılması için altyapı oluşturmaktadır. Kamu kurumları bilgi teknolojileri yönetim sürecini oluştururken, veri tabanı yönetimindeki eksikliklerini, yeni teknoloji önerilerini, bilgi güvenliği farkındalığını denetim fonksiyonunu etkin kullanarak geliştirebilirler.

Bu çalışmada, veri tabanı yönetim sürecine ilişkin denetim fonksiyonu kamu kurumları özelinde ele alınmaktadır.[1] Kamu kurumlarında idari ve teknik alanda ortaya çıkması muhtemel riskler ve bunlara ilişkin bulgu örnekleri üzerinden öneriler geliştirilmekte ve bu önerilerin nasıl izlenmesi gerektiği hakkında görüşler sunulmaktadır.

2. VERİ TABANI YÖNETİM SİSTEMİ

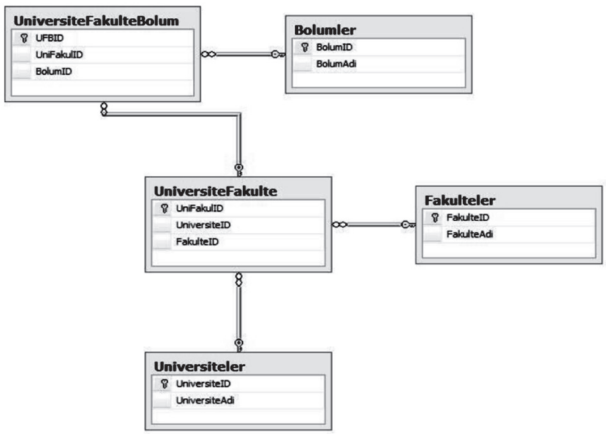
Türk Dil Kurumu güncel sözlüğünde bilgi, "kurallardan yararlanılarak kişinin veriye yönelttiği anlam" olarak tanımlanmaktadır. Tanım içinde geçen "veri" sözcüğü bilginin temel unsurunu temsil etmektedir. Verinin bilgi olabilmesi için tablolama, istatistiksel analiz veya durumun daha iyi anlaşılmasına yol açan başka bir işlemle manipüle edilmesi gerekir (Oz, 2008:9). ISACA terimler sözlüğünde veri tabanı; "işletmelerin ve bireylerin bilgi işleme ve elde etme gereksinimlerini karşılamak için ihtiyaç duydukları ilgili verilerin depolanmış bir koleksiyonudur". Bilgi teknolojilerinin kritik süreçlerinden biri, anlamlandırılarak bilgiyi oluşturacak verinin saklandığı veri tabanlarının yönetimidir. (ISACA, 2018:85)

Veri tabanı yönetim sistemi, büyük veri koleksiyonlarını koruma ve kullanma konusunda yardımcı olmak için tasarlanmış bir yazılımdır. (Ramakrishnan ve Gehrke, 2003:4). Veri tabanı yönetim sistemleri 80'li yıllardan itibaren kullanılmakta ve en genel anlamda dosya tabanlı, ilişkisel (relational) ve ilişkisel olmayan (non-relational) olmak üzere üç ana başlık altında değerlendirilmektedir. Dosya tabanlı veri tabanı yönetim sistemi yönetilmesi en kolay, tek bir dosya içine yazılmış ve sadece gerektiği durumlarda veriye ulaşmak için kullanılan bir sistemdir. Bu yönetim sisteminde ilkel istatistikler dışında herhangi bir bilgi alınamamakta ve günümüzde kullanılmamaktadır ("Types of database", 2014). İlişkisel veri tabanları verilerin satır ve sütunlar içerisinde saklandığı tablolardan meydana gelir. Tablolar belli yapıya uygun verileri saklamak üzere tasarlanır. Bir veri tabanında ilişkiden bahsetmek için en az iki tablo arasında ilişki kurarak, iki tablodaki verileri birbiri ile bağlamamız gerekir. Bu şekilde ilişkisel veri tabanları, veri tabanı olarak adlandırılan büyük dosyalardan oluşur (Sevim, 2005:82). İlişkisel veri tabanı yönetim sistemi ilişkisel veri tabanı oluşturmaya, güncellemeye ve yönetmeye izin veren bir uygulamadır. Veri tabanı yönetim sistemleri kullanıcıların veri tabanından bilgi edinmelerini sağlayacak bir sorgu diline sahiptir. Çoğu ilişkisel

1) Yazarların kamu kurumlarında 10 yılı aşkın süre bilgi işlem departmanındaki ve veri tabanı yöneticiliğindeki görevleri esnasında (hem denetlenen hem de denetim yapan rolleriyle) edindikleri bilgi ve tecrübelerin, ülkemizde mevcut veri tabanı denetimi yazınına aktarımı suretiyle bu denetim türünün geliştirilebilecek yönlerinin ortaya konulmaya çalışılmıştır. Yazıda kaynakçaya atıf yapılmayan bölümler yazarların tecrübe ve görüşlerini yansıtmaktadır.

veri tabanı yönetim sistemleri veri tabanındaki tablolara erişim için SQL (yapılandırılmış sorgu dili) dilini kullanır. SQL, ilişkisel veri tabanı yönetim sisteminde saklanan verilerle iletişim kurmak için kullanılan bir programlama dilidir ("What is a Relational Database", t.y.). SQL ile veri listeleme, kaydetme, güncelleme, silme, veri tabanına yeni bir tablo ekleme, yeni veri tabanı oluşturma veya mevcut veri tabanını değiştirme gibi veri ve veri tabanı yönetimine ilişkin işlemler yapılabilmektedir. Yaygın kullanılan ilişkisel veri tabanları MSSQL, Oracle, MySql, PostgreSql'dir. Şekil 1' de örnek olarak üniversitelerin fakülte ve bölümlerinin kayıtlarını saklayan ilişkisel veri tabanı modeli görülmektedir.

Şekil 1. İlişkisel Veritabanı Örneği



(Unipedi, 2014)

İlişkisel olmayan veri tabanları, verilere erişmek ve verileri yönetmek için belge-tabanlı (Document-Base), grafik tabanlı (Graph-Base), anahtar-değer (Key-Value) ve sütun tabanlı (Column-Base) gibi çeşitli veri modelleri kullanır. Şekil-2'de tiplerine göre ilişkisel olmayan veri tabanları ve örnekleri gösterilmiştir. Anahtar değer veritabanları her veriyi ayrı ayrı anahtarlayarak saklar ve bu anahtar değer ikilisini büyük bir değer tablosu içinde adresler. Belge tabanlı veritabanları, etiketli öğelerden oluşan belgeleri depolar. Sütun tabanlı veri tabanları verileri bir sütundan oluşacak tablolar halinde saklar. Grafik tabanlı veritabanları ise verileri temsil etmek ve saklamak için düğümleri kullanarak bir ağ oluşturur. (Simplilearn, 2019).

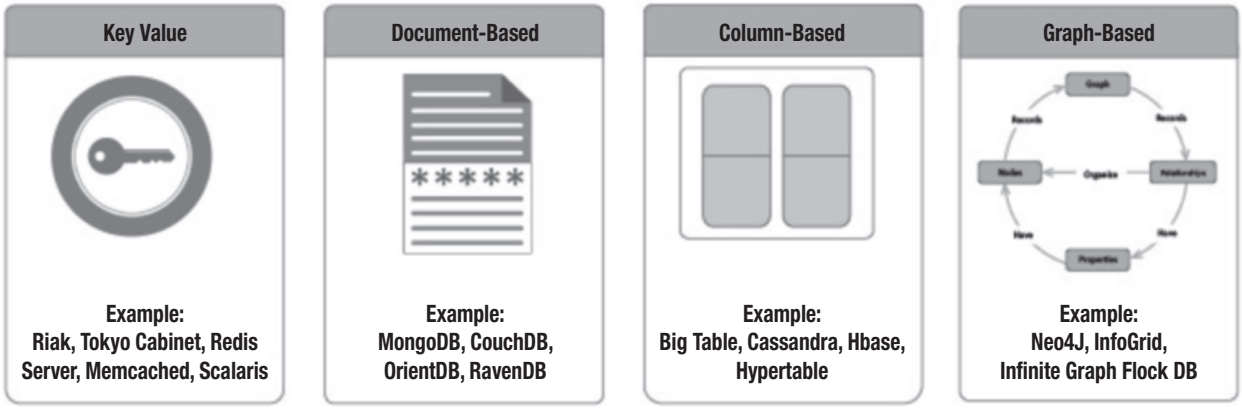
İlişkisel olmayan veritabanları, özellikle büyük veri hacmi, düşük gecikme süresi ve esnek veri modelleri gerektiren uygulamalar için geliştirilmiştir ("NoSQL Nedir", t.y.). Büyük veri (big data) kullanımın artması ve bu büyük veriler üzerinden analiz ve karar destek sistemlerinin geliştirme ihtiyaçlarından dolayı son yıllarda kamu sektöründe ilişkisel olmayan veri tabanlarına ilgi artmaktadır.

Kamu kurumlarında, yaygın bir teknoloji olması ve yönetecek uzman personelin bulunma kolaylığı sebepleriyle, ilişkisel veritabanı kullanımı daha fazla görülmektedir. Veri tabanı yönetimi denetimi incelenirken, kamu kurumlarında daha çok kullanılan ilişkisel veritabanları ön planda tutulmuştur.

3. VERİTABANI YÖNETİMİ DENETİMİ

Günümüzde kamu kurumları hizmetlerini yürütürken yoğun bir şekilde bilgi ve iletişim teknolojileri-

Şekil 2. NoSQL Tipleri



(Simplilearn, 2019)

ni kullanmaktadır. Hizmetlerin etkin ve verimli bir şekilde sunulması adına, veri tabanı yönetim sistemlerinde verilerin güvenli bir şekilde tutulması ve işlenmesi büyük önem arz etmektedir. Veri tabanı yönetim sistemi temel olarak kullanıcılara veri üzerinde düzeltme, ekleme, silme veri tabanı üzerinde ise tasarım, bakım ve erişim gibi işlemleri kolaylaştıran bir yazılımdır (Prabhjot ve Sharma, 2017:362).

Sahip oldukları bilgilerin kritikliği sebebiyle kamu kurumları için veri tabanı yönetimi büyük öneme sahiptir. Risk seviyesi yüksek olan veri tabanı yönetimi belirli periyotlarla denetlenmelidir. Ekip olarak yürütülen bilgi teknolojileri denetimlerinde bütün ekip üyelerinin gerçekleştirecekleri çalışma için uygun seviyelerde yetkinliklere sahip olması, ekip üyeleri arasında görev dağılımı yapılırken her denetim konusu için gerekli profesyonel ve teknik bilgi ve beceriye sahip olan iç denetçinin görevlendirilmesine özen gösterilmelidir (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:16). Mevcut denetçiler arasında teknik yönden yeterli olmayan denetçilerin bulunması halinde konunun uzmanından görüş veya destek alınmalıdır.

3.1. Amaç, Kapsam, Yöntem

İlgili yasal düzenlemelere, talimatlara, politika ve prosedürlere uygun hizmet verilmesi, standart veri tabanı yönetiminin hayata geçirilmesi, varsa süreçte aksayan yönlerin geliştirilerek yürütülen çalışmalara değer katma prensibi veri tabanı yönetimi denetiminin amacını oluşturmaktadır. Bu amaç doğrultusunda kurumlarda veri tabanı yönetimi, yazılım geliştirme, sistem ve ağ yönetimi gibi süreçler; yazılım ve donanım envanteri, yedekleme, bakım, her zaman çevrimiçi, kayıt tutma (logging), denetleme (auditing), gerçek zamanlı izleme, kullanıcı yönetimi stratejileri, test ortamları, veri tabanı standartları, kriz yönetimi konuları kapsamında risk bazlı denetlenmelidir. Bilgi, belge ve dokümanların incelenmesi, süreç sahipleri ile görüşmelerin yapılması, sürecin gözlenmesi ve teknik incelemeler başlıca denetim yöntemini oluşturmalıdır.

3.2. Risklerin Belirlenmesi ve Ön Çalışma

Denetlenen kurum için veri tabanı yönetimi sürecindeki muhtemel riskler belirlenmelidir. Ön çalışma sırasında, riskleri belirlemek için, ilgili mevzuatları ve iyi uygulama örnekleri (best-practice) incelenmeli, mevcutta olması gereken durum belirlenmelidir. Bu kapsamda, *Kişisel Verileri Koruma Kanunu, KamuNet Tebliği, E-Devlet Hizmetlerinin Yürütülmesine İlişkin Usul Ve Esaslar Hakkında Yönetmelik ve ISO 2700x Bilgi Güvenliği Standartları* gibi bilgi teknolojileri ile ilgili mevzuat, hizmet alım sözleşmeleri ve denetlenecek kurumun teşkilat ve görevleri ile ilgili kanun, yönetmelik, genelgeler ve talimatlar incelenmelidir. Yine ön çalışma sırasında kurumun teşkilat yapısı incelenmeli, veri tabanı yönetim sürecinden sorumlu birim belirlenmeli ve saha çalışması yapılmadan önce birim yöneticisi ve personel ile ilgili bilgi toplanmalıdır. (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:27). İlgili birimlerden personel görev dağılımları, sorumlulukları ve eğitim durumları, yazılım ve donanım envanterleri, yedekleme, bakım gibi süreçlere ilişkin yazılı politika, prosedürler ve eylem planları istenmelidir.

Kamuda veri tabanları yönetimi denetimi yapılırken, risklerin belirlenmesi için yapılacak çalışmalar idari ve teknik olarak iki grupta sınıflandırılabilir. Riskler belirlenirken bilgi güvenliği unsurları da göz önünde bulundurulmalıdır. McCumber bilgi güvenliğini "Bilgi ve bilgi sistemlerinin yetkisiz erişimi, kullanımı, ifşa edilmesi, bozulması, değiştirilmesi veya bilginin gizlilik, bütünlük ve kullanılabilirliğine zarar vermek için yapılan kötü niyetli girişimlere karşı sağlanacak koruma" şeklinde tanımlamaktadır (McCumber, 2005:xxiii). McCumber Bilgi Güvenliği Modeli'ne göre bilgi, "gizlilik", "bütünlük" ve "erişilebilirlik" olarak isimlendirilen üç temel unsurdan oluşur (McCumber, 2005:136).

- Gizlilik, bir bilgiye erişimi uygun görülen kişilerin bilgiye erişiminin sağlanmasıdır (Henkoğlu ve Yılmaz, 2013:455).
- Bütünlük, verinin yetkisiz kişiler tarafından değiştirilmesi silinmesi ya da herhangi bir şekilde tahrip edilmesi tehditlerine karşı içeriğinin korunmasıdır.
- Erişilebilirlik, kullanıcının ihtiyacı olan bilgiye yetkisi dahilinde ve istediği anda ulaşabilmesidir (Henkoğlu ve Yılmaz, 2013:455).

Teknik riskler; süreçte kullanılan bilgi teknolojilerinin yeterli, güncel, güvenli olması, sistem yapılandırması, uygulama erişim, yetki, konfigürasyon kontrolleri olup, bu hususlar bilgi güvenliğine ilişkin McCumber

tarafından belirlenen unsurlarda dikkate alınarak incelenir. İdari riskler ise; süreçlerden sorumlu birimlerin yönetim, mevzuat açısından ve süreç sorumlularının yetkinliği bakımından incelenmesi ile belirlenir.

Saha çalışması sırasında olası risklerin oluşturacağı bulguların tespiti için bu ayrıma dikkat edilmesi gerekir. Veri tabanında çalışan teknik personeli, yönetim veya mevzuatla ilgili konularda teste tabi tutmak zaman kaybına yol açıp doğru bilgiye ulaşmayı engelleyecektir. Aynı şekilde yönetim kadrosunu, teknik konularla değerlendirmek risklerin tespitinde zorluklara yol açacaktır. Bu kapsamda denetim ekibi oluşturulurken, idari ve teknik risk kategorilerinin olacağı göz önünde bulundurulmalıdır.

Kamu kurumlarındaki veri tabanları yönetim süreci için idari riskler;

- Veri tabanı yönetiminden sorumlu birime, görevler ayrılığı ilkesine aykırı verilecek diğer görevler nedeniyle hata ve usulsüzlüklerin tespit edilememesi ve hizmetlerin aksaması,
- Veri tabanlarından sorumlu personelin görev tanımlarının yapılmamış olması nedeniyle mükerrer görevlerin ortaya çıkması veya açıkta görev kalması,
- Mevzuat ile tanımlanmış görevlerin uygulama ile uyuşmaması sebebiyle yetki ve sorumluluk karmaşası yaşanması ve hizmetlerin aksaması,
- Yetkin olmayan teknik personel görevlendirmesi nedeniyle veri kayıplarının yaşanması ve bilgi güvenliği açıklarının oluşması,
- Farklı veri tabanı yönetim sistemlerine ve yeni teknolojik gelişmelere ilişkin personel eğitim ihtiyaçlarının karşılanmaması nedeniyle personelin yönetimde yetersiz kalması ve veri tabanlarının etkin yönetilememesi,
- Kriz anı eylem planlarının oluşturulmaması nedeniyle olaylara zamanında müdahale edilememesi ve hizmetin kesintiye uğraması,
- Güncel yazılım ve donanım envanteri tutulmaması nedeniyle ihtiyaç fazlası alımların yapılması, kullanılmayan yazılım ve donanımların tespit edilememesi ve kaynakların etkin kullanılamaması,
- Veri tabanı yönetiminden sorumlu birim ile diğer birimler arasındaki iletişim problemleri nedeniyle sistem, uygulama ve donanım hatalarının kaynağının tespit edilememesi ve hizmetlerin aksaması,
- Kurumda, veri tabanı yönetiminden sorumlu birimin kontrolü dışında veri tabanı yönetimi yapılması nedeniyle mükerrer yatırımların olması, standart veri tabanı yönetimi sağlanamaması, kaynakların etkin kullanılmaması ve bilgi güvenliği açıklarının oluşması,
- Kurum veri tabanı standartlarının belirlenmemesi nedeniyle anlamsız isimlendirmelerin ve kısaltmaların oluşturulması, veri tabanı kullanıcılarına atanan rol ve sorumlulukların eksik veya fazla olması, veri tabanı yöneticisi ile uygulama geliştiricileri arasında anlaşmazlıkların yaşanması, veri tabanı güvenliğinin yeterli düzeyde sağlanamaması,

şeklinde belirlenebilir. İdari açıdan oluşabilecek muhtemel riskler sorumlu birim yönetimi, mevzuatı ve personeli hakkında bilgi edinildikten sonra güncellenmelidir.

Teknik riskler ise;

- Yedekleme stratejisinin belirlenmemesi nedeniyle eksik yedekleme alınması, yedekten veri kurtarma işleminin yapılamaması ve hizmetin kesintiye uğraması,
- Bakım planlarının (maintenance plan) tanımlanmaması nedeniyle veri tabanı sürekliliğinin sağlanamaması, performansının azalması ve veri kayıplarının yaşanması
- Her zaman çevrimiçi (always on) mimarisinin oluşturulmaması nedeniyle sunulan hizmetlerin kesintiye uğraması sonucunda imaj ve itibar kaybı yaşanması,
- Veri değişim kayıtlarının (log) standartlarının belirlenmemesi nedeniyle anlamlı olmayan kayıtların oluşması ve ihtiyaç duyulan kayıtların bulunmasında zaman kaybı yaşanması,
- Denetim kayıtlarının (audit log) tutulmaması nedeniyle veri tabanı üzerinde değişiklik yapan kullanıcıların tespit edilememesi ve bilgi güvenliği açıklarının oluşması,
- Gerçek zamanlı izlemenin (real-time monitoring) yapılmaması nedeniyle sistem sürekliliğinin ve güvenliğinin sağlanamaması,
- Kullanıcı erişim ve yetkilendirme kontrollerinin belirlenmemesi nedeniyle verilerin yetkisiz kişilerin eline geçmesi ve bilgi güvenliği açıklarının oluşması,

- Canlı (production), test ve geliştirme (development) ortamlarının birbirinden ayrı oluşturulmaması nedeniyle verilerin değiştirilmesi ve sorumlunun tespit edilmemesi,
- Test ve geliştirme ortamlarında gerçek verinin kullanılması nedeniyle veri sızıntılarının olması ve bilgi güvenliği açıklarının oluşması,

şeklinde sıralanabilir.

Belirlenen bu riskler denetim ekibi tarafından test edilerek varlığı, etki ve olasılıkları kontrol edilmelidir.

3.3. Saha Çalışması, Testler, Öneriler

Saha çalışmasında olması gereken durum ile mevcut durum arası farklar test edilmeli ve test sonuçlarından elde edilen bilgiler kayıt altına alınmalıdır. Testlerin uygulanması sonucu elde edilen bilgilerin; yeterli, güvenilir, ilgili, faydalı olması gerekir (Kamu İç Denetim Rehberi, 2013:55). Saha çalışması sonunda denetim ekibi test sonuçlarını incelemeli uygunsuzluk tespit ettiği durumları bulguya çevirerek gerekli önlemler veya düzeltmeler için öneri geliştirmelidir.

Saha çalışması sırasında uygulanacak testler; konusuna göre birebir görüşme, evrak inceleme veya teknik inceleme şeklinde olabilir. Saha çalışması öncesi belirlenmiş olası riskler için yapılacak test konuları dışına çıkılmamaya dikkat edilerek gerçekleştirilmeli ve net bilgiye ulaşılmaya çalışılmalıdır. Yapılan her test bir konuya özel olmalı ve çalışma kağıtlarına test içeriği kayıt edilmelidir. Denetim süresinin verimli kullanılması ve saha çalışmasının etkin planlanması için olası risklerin idari ve teknik olmak üzere iki kategoriye ayrılmasının uygun olacağı düşünülmektedir.

3.3.1. İdari Riskler

İdari risklerin etkisini kontrol için yapılacak testler, genel olarak görüşme ve evrak incelemesi şeklinde olmaktadır. Bu aşamada riskler ve etkileri incelenip olası senaryolar üzerinde durulacaktır.

İdari risklerin tespiti için, saha çalışması başlamadan önce kurumun mevzuatı incelenmeli ve veri tabanı yönetimi ile ilgili görevlerin hangi birime verildiği tespit edilmelidir. Bu birimlerin iş süreçleri incelenmeli ve yeterliliği kontrol edilmelidir. (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:27). Kurum mevzuatında veri tabanı yönetimi ile ilgili görevlerin hangi birime verildiğinin belirlenmemiş olduğu tespit edilmişse, sürecin sorumlusunun net olarak belli olmadığı sonucu çıkarılarak bulgu olarak kaydedilmesi gerekir. Bu durum için veri tabanı yönetim süreci sorumluluğunun hangi birime verildiğinin açık şekilde belirlendiği mevzuat çalışması önerilmelidir.

Veri tabanı yönetim sürecinden sorumlu birim tespit edildikten sonra personel bazlı görevlendirmelerin olup olmadığı incelenmelidir. Yedekleme, bakım, gerçek zamanlı izleme gibi kritik işlerden sorumlu personelin tanımlı olması, kişi sayısı fazla olan birimlerde yönetimsel olarak kolaylık sağlayacağı gibi görev karmaşasının da önüne geçecektir. Görev tanımı yapılmış her personelin en az bir yedeğinin belirlenmiş olması iş sürekliliğini sağlama açısından önemlidir. Test esnasında personel görevlendirmelerinin yazılı olarak varlığı incelenmeli, var olduğu görülse dahi görevlendirilmiş personelin görevlerini bilip bilmediği ve görevlendirmesi kapsamında yaptığı çalışmalar sorgulanmalıdır. Görev tanımlarının ve personel yedeklerinin olmadığı tespit edildiğinde, gerekli düzenlemelerin yapılarak personele tebliğ edilmesi önerilmelidir.

Görevler ayrılığı ISO 27001:2013 standardında "*Kuruluşun varlıklarının yetkisiz veya farkında olmadan değiştirilme ya da kötüye kullanılma fırsatlarını azaltmak için, görevler ve sorumluluk alanları ayrılmalıdır.*", Kamu İç Kontrol Standartlarında ise *"Hata, eksiklik, yanlışlık, usulsüzlük ve yolsuzluk risklerini azaltmak için faaliyetler ile mali karar ve işlemlerin onaylanması, uygulanması, kaydedilmesi ve kontrol edilmesi görevleri personel arasında paylaştırılmalıdır.*" şeklinde düzenlenmiştir (Kamu İç Kontrol Standartları, 2007:9). Saha çalışması sırasında düzenlemelerle birimlere ve kişilere tanımlanmış görevlerin uygulamada gerçekleştirilip gerçekleştirilmediği incelenmelidir. Birimlerin tanımlanmış görevlerini yerine getirmediği, sözlü talimatlarla görevi olmadığı halde başka birime tanımlı görevleri ifa ettiği tespit edildiğinde ya görev tanımlarında değişiklik yapılması ya da yerine getirilen görevin ilgili birime devredilmesi önerilmelidir.

Gelişen teknoloji ve hemen her alanda bilgisayar kullanımı, emek yoğun üretimden otomasyona geçişin hızlanması, birçok alanda uzmanlaşmanın öneminin artması ve insan ihtiyaç ve beklentilerindeki değişim,

yeni bazı işlerin ve meslek alanlarının doğmasına yol açmaktadır. (Köklü, 2018:121) Veri tabanı yönetimi de oldukça teknik ve uzmanlık gerektiren bir konudur. Kamu kurumlarının günümüzde özellikle bilişim alanında hizmet alımı veya sözleşmeyle teknik personel çalıştırdığı bilinmektedir. Bu yöntemlerle veri tabanı yöneticisi olarak istihdam edilecek kişilerin yetkinlikleri tam olmalıdır. Kamu kurumlarının veri tabanı yöneticilerini hizmet alımı veya sözleşme yöntemiyle istihdam etmesinin başlıca sebebinin, bu süreci yönetecek kamu personelinin bulunmaması ve uzman personel ihtiyacı olduğu unutulmamalıdır. Test esnasında bu yöntemle istihdam edilmiş personelin işe alım kriterleri, eğitim durumu, uzmanlık alanıyla ilgili sertifikaları, geçmişte çalıştığı projeler, etik sözleşmesi ve kurum tarafından bedeli ödenmiş eğitim alıp almadığı incelenmelidir. Bu yöntemle alınacak veri tabanı yöneticisi alım kriterlerinde eksiklik olması durumunda ulusal mesleki yeterlilik standardında belirtilen veri tabanı yöneticisi kriterlerine uyulması önerilmelidir.

Kamu personeli olup veri tabanı yönetimiyle görevlendirilmiş personelin yetkinliği kritik öneme sahiptir. Her ne kadar günümüzde kamu kurumları bilişim alanında sözleşmeli ve hizmet alımıyla personel çalıştırmayı tercih etseler de bu yöntemin kalıcı çözüm üretmeyeceği aşikârdır. Sözleşmesi sona eren personelin kurumda çalışmaya devam etmesi kesin olmayıp, veri tabanı yönetimi gibi kritik bir görevin sadece hizmet alım yöntemiyle sürdürülmesi bilgi güvenliği açısından düşünülemez.Personel bulma ve seçme sürecinde hangi teknik kullanılırsa kullanılsın, işe tam uyumlu hazır bir çalışan bulmak oldukça güçtür. Bu zorluğun getirdiği eksiklikleri gidermenin en iyi yolu eğitimdir. (Muradova, 2007:77) Kamu kurumlarında çalışan personeller arasında da veri tabanı yöneticisi olarak çalıştırılacak yetkinlikte personel bulmak zordur. Veri tabanı yöneticisi olarak çalışan personel mevcudiyeti ve yetkinliği incelenmeli, mevcut değilse görevlendirilmesi, yetkinliği ile ilgili problem varsa kurumun kullandığı veri tabanı sistemiyle ilgili eğitim aldırılması önerilmelidir.

Günümüzde kamu kurumları bilişim hizmetleri vatandaş odaklı geliştirilmektedir. E-devlet uygulamaları ile vatandaşlara 24 saat kesintisiz hizmet verme politikası yürütülmektedir. Bu politika, veri tabanlarının 24 saat hizmet vermesi zorunluluğunu ortaya çıkarmaktadır. Bu sebeple veri tabanlarında oluşabilecek hatalar vatandaşa ve paydaş kurumlara yapılan paylaşımın aksaması yanında, kurum tarafından verilen hizmetlerde de aksamaya yol açacağından kriz durumunun oluşmasına neden olacaktır. Bilgi teknolojileri hizmetlerinde oluşan beklenmedik kesintiler veya hizmet kalitesinin düşmesine sebep olacak durumlar "olay" olarak değerlendirilmektedir. (Kamu Bilgi Teknolojileri Denetimi Rehberi, 2014:129). Olay anlarında yapılacak işlemlerin önceden planlanması ve görevli personelin belirlenmesi gerekmektedir. Bu durumunun ne zaman olabileceği tahmin edilemeyeceğinden 24 saat esasına göre olay yönetim planı oluşturulmalıdır. Saha çalışması sırasında olay yönetim planının olup olmadığı ve uygulanabilirliği incelenmelidir. Olay yönetimi planı içinde görevlerin net tanımlanması ve müdahale edecek personelin belirlenmesi, mesai saatleri dışında oluşabilecek kriz anları için müdahale edecek personelin nöbet sistemi oluşturularak haftalık veya aylık dönüşümlü görevlendirilmesi önerilmelidir.

Bilgi teknolojileri ürünleri kuruma maddi olarak büyük yük getirmektedir. Kamu kurumları ihtiyaç duydukları kaynakları belirleme konusunda dikkatli davranmalıdır. Kaynak ihtiyaçlarının tespiti mevcut varlıkların iyi yönetilmesi ile mümkün olabilir. Veri tabanı yönetim sürecinde kullanılan sunucular, veri tabanı güvenlik duvarları (database firewall), depolama üniteleri (storage), yedekleme üniteleri (backup device), ağ araçları (network tools), yazılım lisansları ve kullanım durumları kayıt altına alınmalıdır. Bu kontrol sayesinde kaynak ihtiyaçlarının belirlenmesi daha verimli hale getirilmiş olacaktır. Veri tabanı yönetiminden sorumlu birimlerin envanterinin düzenli tutulup tutulmadığı ve güncelliği incelenmelidir. Mevcut veya güncel olmaması halinde kaynakların etkin kullanımı için donanım ve yazılım envanterinin takip edilebileceği *(lisans, versiyon, garanti süresi, teknik özellik, kaynak kodları, sorumlu personel, IP, marka, model vb. kriterleri içeren*) bir uygulama geliştirilmesi veya temin edilmesi ve envantere eklenecek veya envanterden çıkarılacak yazılım ve donanımların anlık olarak güncellemesinin sağlanması önerilmelidir.

Yaptıkları işin mahiyeti itibariyle farklılık gösteren birimler birbirlerinden bağımsız olarak çalışmalı ve yetki ve sorumlulukları net olarak tanımlanmalıdır.

(Koçel , 1982:237).Yazılım geliştirme, veri tabanı yönetimi, bilgi güvenliği ve sistem yönetimi süreçleri görevler ayrılığı ilkesine uyularak farklı birimlerde yönetilmeli ve bu süreçlerin birbirleri ile olan ilişkisinden dolayı birimlerin yatay iletişiminde aksama yaşanmamalıdır. Bilgi işlem hizmeti tüm bu süreçlerin koordineli şekilde çalışmasıyla verimli yönetilebilir. Veri tabanı yönetimi ile ilgili birim denetlenirken diğer birimlerle de görüşülmeli, birimler arası yaşanan problemler tespit edilmelidir. Tespit edilen problemlerin içeriğine göre bağlı oldukları üst yöneticiye bilgi verilip, her birimin görevi dikkate alınarak iletişim yollarını kolaylaştırıcı, resmi yazışmaların en aza indirilip kurumsal eposta yoluyla veya kurulacak bir sistemle isteklerin elektronik ortamda alındığı, cevaplandığı ve kaydedildiği bir sistemin kullanılması önerilmelidir.

Kamu kurumlarında bilgi işlem birimleri yardımcı hizmetler olarak tanımlanmaktadır. Kurumun asli görevlerine yardımcı olacak şekilde bilgi teknolojileri altyapısını oluşturmakla görevlendirilmiştir. Kurumların asli görevlerini yerine getiren birimler günümüz teknolojilerine ayak uydurmak, vatandaşa daha iyi hizmet sunmak amacıyla bilgi teknolojileri projeleri üretebilmektedir. Bazı durumlarda üretilen bu projeler hizmet alımı yöntemleri kullanılarak temin edilmekte, bilgi işlem birimlerinin bilgisi olmadan kurum içinde farklı yerlerde veri tabanı yönetimi yapılabilmektedir. Bu durum kaynakların verimli kullanılmasına engel olmaktadır. Farklı birimlerde bulunan veri tabanları, merkezi veri tabanları için oluşturulan yedekleme, bakım, kriz (olay) yönetimi, kapasite ihtiyaç tespiti gibi stratejilerden faydalanamamaktadır. Kurumda kullanılan tüm uygulamaların tespit edilmesi ve veri tabanlarının yönetiminin veri tabanı yönetim birimine alınmasının sağlanması, bundan sonra geliştirilecek uygulamalarda merkezi veri tabanı altyapısının kullanılmasını zorlayıcı önlemler alınması önerilmelidir.

Kamu kurumlarında süreçlerin standartlarının konulmaması ve dokümantasyonunun yapılmaması, kişi bağımlılığı yaratmakta ve sonucunda yönetim riski oluşmaktadır. Personel bağımlılığı olan işler kişiyle özdeşleşerek başkası tarafından yürütülemeyecek duruma gelebilmektedir. "Standartlar ve prosedürler, süreçler üzerinde daha fazla kontrol sahibi olmanızı sağlar. Tasarım kararları için oluşturulacak yönergeler ile uygulama ve veri tabanı tasarımında verimlilik artar. Açıkça tanımlanmış sorumluluklar sayesinde uygulama geliştiricileri ve veri tabanı yöneticileri arasındaki iletişim gelişir. İşletim prosedürleri ile işlemlerde güvenilirlik artar." ("Standards and procedures", t.y.). Riskin bulguya dönüşmesi halinde veri tabanı yönetim süreci için kurum standartlarının (isimlendirme, kullanıcı, dokümantasyon, teknoloji standartları gibi) oluşturulması önerilmelidir.

3.3.2. Teknik Riskler

Teknik risklerin etkisini kontrol için yapılacak testler, genel olarak görüşme, teknik inceleme ve yerinde izleme şeklinde olmaktadır. Bu yöntemlerin uygulanması aşağıda detaylandırılmaktadır.

Bilgi sistemlerinin erişilebilir olmasını sağlayan profesyoneller tarafından, veri depolama alanlarının her an güncel bilgi ile kullanıcıyı buluşturması noktasında üstlenilen kritik sorumluluk; aktif olarak hizmet veren cihazların altyapı yedekliliği ve yeterliliğinin yanı sıra veri yedekliliğinin de düzenli olarak yapılması ve gerektiğinde en kısa sürede hizmete sunulmasını zorunlu kılmaktadır (Henkoğlu ve Yılmaz, 2013:456). Bu nedenle veri tabanları için yedekleme ve bakım stratejileri kritik öneme sahiptir. İlişkisel veri tabanı yönetiminde yedekleme tam (full backup), fark (differential backup) ve işlem (transactional backup) yedeklemesi olarak üç ana başlık altında toplanmaktadır. Veri tabanı yöneticisi, yönettiği veri tabanının kritikliğine, boyutuna ve sakladığı veriye ilişkin yasal mevzuatına göre yedekleme periyotlarını ve yedeklerin saklanma süresini belirlemelidir. Otomatik yedekleme görevleri günlük olarak kontrol edilmeli, belirli periyotlarla yedekten geri dönüş testleri yapılıp kayıt altına alınmalıdır. Saha çalışması sırasında yedekleme stratejisi incelenmeli, geçmişe dönük yedekleme görevlerinin başarıya ulaşıp ulaşmadığı ve yedekten geri dönüş testlerinin kayıtları kontrol edilmelidir. Yedekleme için kullanılan yedekleme üniteleri belirli periyotlarda kapasite ve hatalara karşı kontrol edilmeli, zamanlanmış yedekleme planlarının doğru çalışıp çalışmadığı günlük olarak izlenmeli ve yedeklerin büyüklüğü ve kritikliği göz önüne alınarak yedekten geri dönüş testleri yapılmalıdır. Yedekleme stratejisinin tüm veri tabanlarını kapsayacak şekilde oluşturulması ve yedekten geri dönüş testlerinin rutin

olarak yapılması ve kayıt altına alınmasının talimatlandırılarak yazılı hale getirilmesi önerilmelidir.

Bakım planları (maintenance plan) veri tabanlarının performansı açısından kritik öneme sahiptir.Bakım planları, veri tabanı kritiklik, büyüklük ve kullanım sıklığı gibi kriterler göz önünde bulundurularak yapılmalıdır. Özellikle anlık işlem (transaction) sayısı fazla olan uygulamalarda veya kayıt sayısı fazla olan tablolardan sorgulama yapılırken performans kayıpları, darboğazlar veya sistem çökmeleri yaşanmaması açısından bakım planları önem arz etmektedir.Bakım planları için oluşturulan otomatik görevler, uygulamaların aktif kullanıldığı saatler dışında çalışacak şekilde ayarlanmalıdır. Özellikle ilişkisel veri tabanı kullanan kurumlarda indeks ve istatistiklerin yeniden oluşturulması, bakımları sistemi yormayacak zamanlarda planlanıp uygulanmalıdır. Bakım stratejisinin tüm veri tabanlarını kapsayacak şekilde oluşturulması ve talimatlandırılarak yazılı hale getirilmesi önerilmelidir.

Her zaman çevrimiçi (Always on) mimarisi, aktif çalışan veri tabanlarının plan dışı durması sonucu, kendisiyle eş zamanlı (senkron) çalışan ikinci bir sunucunun devreye girip sistem devamlılığının sağlanması için kullanılmaktadır. İşletim sistemi bazlı olabileceği gibi veri tabanı sunucusu bazlı olarak da kurgulanabilir. Veri tabanını kullanan uygulamaların teknolojik bağımlılıkları da dikkate alınarak otomatik yük devretme (automatic failover) tasarımın içine dahil edilebilir. Her zaman çevrimiçi mimarisi kurumun ihtiyaçları doğrultusunda tasarlanmalı kaynak israfına sebep olmamalı ve belirli periyotlarla birincil sunucu değiştirme testleri yapılmalıdır. Saha çalışmasında her zaman çevrimiçi mimarisinin varlığı sorgulanmalı, yoksa önerilmeli, varsa yük devretme (failover) testlerinin kayıt altına alınması, sistemlerin kritikliğine göre otomatik yük devretme fonksiyonlarının aktifleştirilmesi önerilmelidir.

Günümüz veri tabanı yönetim sistemlerinde bilginin bütünlüğünü korumak ve yetkisiz değişimini tespit etmek için log (kayıt) tutulmaktadır. Veri tabanı içerisinde saklanan verilerin uygulama içinden değiştirilmesi veya silinmesi kayıtlarını uygulamanın kendisi yapması gerekmektedir. Bu kapsamda veri tabanı yönetimine düşen bir görev olmadığı görülse de kurum içinde birçok farklı uygulama olduğu düşünüldüğünde ve bu uygulamaları geliştiren firma veya yazılım geliştiricilerin farklı olmasından dolayı kayıt tutma tasarımları farklı olacaktır. Kamu kurumları bu kayıtlara çoğunlukla adli makamlardan gelen sorular üzerine ulaşmakta ve doğru bilgiyi vermek zorundadır. Bu kapsamda kayıtların (loglar) merkezi bir kayıt sisteminde bulundurulması veya veri tabanı yönetimi tarafından standartlaştırılmış bir formatta tutulması gerekmektedir. Kurumun merkezileştirilmiş veya standartlaştırılmış bir kayıt tutma mekanizması olup olmadığı sorgulanmalı, yok ise kayıtlar için bir standart oluşturulması, kayıt altına alınması gereken asgari verilerin (tarih, ip, sorgu, kullanıcı gibi) belirlenmesi ve yeni geliştirilecek uygulamalarda belirlenen standartlara uyulmasının sağlanması önerilmelidir.

Veri tabanı içinde saklanan verilerin değişimi için tutulan kayıtlardan (log) daha önce bahsedilmişti. Bir diğer değişim izleme mekanizması ise denetim (audit) kayıtlarıdır. Denetim kayıtları (auditing) seçili veri tabanları üzerinde yapılan işlemleri izleme ve kaydetme sistemidir. (Oracle, 2019). Daha önce açıklanan McCumber Bilgi Güvenliği Modeli'ne göre bilginin üç temel unsurundan biri olan bütünlük verinin yetkisiz kişilerce değiştirilmesidir. Veritabanı üzerinde yapılan mimari değişiklikler, tanımlanan veya silinen görevler (job), tanımlanan, silinen veya yetkilendirilen kullanıcılar denetim kayıtlarıyla saklanmalıdır. Bu sayede veri tabanı üzerinde yapılan tüm değişiklik işlemleri kayıt altına alınmış olur. Saha çalışması sırasında denetim kayıtları (audit) saklama stratejileri incelenmelidir. Tüm veri tabanları için sunucu tarafı değişim işlemleri, kullanıcı değişim işlemleri, veri tabanları için oluşturma (CREATE), değiştirme (ALTER), silme (DROP) işlemleri ve başarısız giriş (FAILED_LOGIN) işlemlerinin kayıtlarının açılması önerilmelidir.

Veri tabanlarının güvenliğinin sağlanması ve sistemin sürekliliği açısından gerçek zamanlı izlemenin yapılması büyük öneme sahiptir. Gerçek zamanlı izleme yaparak iç ve dış kullanıcılar tarafından gelebilecek olan saldırılara karşı önlem alınmış olur. Ayrıca veri tabanı yönetim sisteminde gerçekleşebilecek olağandışı durumlar tespit edilerek sistemin devamlılığı sağlanmalı, sistemde meydana gelecek hatalar anlık olarak uyarı sistemi aracılığı ile veri tabanı yöneticilerine sms veya e-posta olarak bildirilmelidir. Veri tabanı sunucularının kullandığı depolama birimi

(disk), işlemci (cpu), bellek (ram) anlık takip edilmeli, eşik değerler belirlenmeli ve bu değerlerin aşılması durumunda alarm üretmelidir. Test esnasında böyle bir izleme ve uyarı sisteminin varlığı kontrol edilmeli varsa geçmişte ürettiği alarmlar incelenerek yeterliliği incelenmelidir. İzleme ve uyarı sistemi bulunmuyorsa kurumun ihtiyaçlarına ve sistemlerin kritiklik durumlarına göre izlenmesi gereken kaynaklar belirlenerek izleme sisteminin geliştirilmesi önerilmelidir.

Veri tabanları kurum içinde kullanılan tüm veriyi saklaması ve veri üzerinde değişiklik yapılabilmesi için tasarlanmıştır. Yetkilendirme, şifre ile erişim ve veri kriptolama işlemleri; bilgi gizliliğinin sağlanması için kullanılan başlıca yöntemlerdir (Henkoğlu ve Yılmaz, 2013:455). Verinin veya verinin içinde bulunduğu tablo (sql tabanlı) ya da dokümanın (no-sql tabanlı) yapısal olarak değiştirilmesi, belirlenmiş bir kimlik doğrulama (authentication) ve yetkilendirme (authorization) prosedürü aracılığı ile yapılmalıdır. Geliştirme, test ve uygulama ortamlarındaki yetkilendirme ve kimlik doğrulama kuralları ayrı ayrı belirlenmeli ve duyurulmalıdır. Geliştirme ortamlarında yazılım geliştiricilere geniş yetkiler verilebilirken test ve uygulama ortamlarında kısıtlı yetkiye izin verilmelidir. Bu kapsamda veri tabanları üzerinde erişim, okuma veya yazma izinleri olan tüm kullanıcılar incelenmeli bu yetkilerin neden verildiği araştırılmalıdır. Sistem yöneticisi yetkisine sahip kullanıcılar ayrıca incelenmeli gereksiz yetkilendirmelerin olup olmadığı kontrol edilmelidir. Varsayılan olarak tanımlanmış sistem yöneticisi kullanıcılarının (MSSQL için sa, PostgreSQL için postgres gibi) pasif hale getirilmesi, tüm kullanıcılar için (uygulama, yönetici, geliştirici vb.) parola politikası belirlenmesi ve sistemsel olarak uymaya zorlanması, tespit edilen gereksiz yetkili kullanıcıların silinmesi önerilmelidir.

Veri tabanı yönetiminde geliştirme, test ve uygulama veri tabanı ortamlarının birbirinden ayrılması ve etkin şekilde kullanılması önem arz etmektedir. Geliştirme ortamı yazılım geliştiricilerin kullandığı veri tabanı üzerinde, uygulamanın geliştirilmesi sırasında gerekli olacak her türlü tasarım ve mimari değişikliklerini yapabileceği fakat içerisinde gerçek verilerin bulunmayacağı ortamdır. Test ortamı, uygulamanın canlı olarak devreye alınmadan önce uygulama ortamıyla hemen hemen aynı özelliklere sahip sunucu içinde test edilmesine olanak sağlayacak, içerisinde gerçek verinin hiç bulunmadığı ya da sadece tanım tablolarının ve kritik olmayan verinin bulunabileceği ortamdır. Verilerin güvenliğini sağlamak üzere test ortamında yazılım geliştirici ve uygulama kullanıcısı kısıtlı yetkiye sahip olmalıdır. Uygulama ortamı ise tüm güvenlik önlemlerinin alındığı, uygulama kullanıcısına sadece gerektiği kadar yetki verilen, yazılım geliştirici kullanıcısına ise yetki verilmemiş canlı ortamı ifade etmektedir. Kaynak planlaması yapılırken geliştirme ortamı için yedekleme ve bakım hizmetleri göz ardı edilebilmektedir. Test ve uygulama ortamları için bakım ve yedekleme hizmetleri verilmelidir. Saha çalışması sırasında bahsedilen bu ortamların varlığı incelenmeli, yok ise nedenleri araştırılmalıdır. Özellikle geliştirme ve test ortamlarında kullanılan test verilerinin gerçek olup olmadığı kontrol edilmelidir. Uygulama ortamı için alınan güvenlik tedbirlerinin test ortamı için alınmaması, test ortamındaki yetkilendirmelerin uygulama ortamındaki yetkilendirmelerden farklı olması gibi nedenlerle test ortamında gerçek verinin bulunması bilginin gizliliği ilkesinin ihlali ile sonuçlanabilir. Ortamların yaratılması için gerekli maliyetlerde göz önünde bulundurularak kurumun ihtiyaçları doğrultusunda geliştirme, test ve canlı ortamların oluşturulması, canlı ortam hariç hiçbir ortamda gerçek verinin bulunmamasının sağlanması, her bir ortam için kullanıcı yetki standartlarının belirlenmesi önerilmelidir.

Yapılan testler sırasında kısa sürede müdahale edilerek düzeltilebilecek tespitler bulunması halinde tespit edilen durumun düzeltilmesi önerilmeli ve bu husus raporda belirtilmelidir.

3.4. İzleme

Denetimin en önemli aşamalarından biri olan izleme faaliyeti etkin bir şekilde uygulanmalıdır. Saha çalışması sırasında riskli alanlar için yapılan testler sonucunda oluşturulan ve denetlenen birim ile hemfikir olunan bulguları önlemek ve düzeltmek için geliştirilen öneriler için makul gerçekleştirme tarihleri belirlenmelidir. Denetlenen birim tarafından belirlenecek bu tarihler bulgunun risk seviyesi, denetlenen birimin kaynak durumu göz önüne alınarak oluşturulmalıdır.

Bulguyu bertaraf etmek için oluşturulmuş öneriler yerine getirilmiş ise bulgu kapatılmalıdır. Öneriler zamanında yerine getirilmemiş ise nedenleri araştırılmalı, yerine getirilmeme sebebinin zorunluluktan mı kaynaklı olduğu belirlenmelidir. Denetlenen birimin bulguyla ilgili yaptığı çalışmalar görülmüş ise süre uzatımı verilmelidir. Eğer denetlenen birimin öneri ile ilgili yaptığı veya devam eden bir çalışması yok ise ve ilave süre istememiş ise riskin denetlenen birim tarafından üstlenildiği ile ilgili bilgilendirme kendilerine ve üst yöneticiye yapılmalıdır. Risklerin belirlenmesi ve saha çalışmasında yapıldığı gibi izleme faaliyetinin de idari ve teknik olarak iki başlıkta yapılması halinde izlemenin daha etkin yürütülebileceği düşünülmektedir.

3.4.1 İdari Risklerin Oluşturduğu Bulguların İzlenmesi

Veri tabanı yönetiminden sorumlu birimin ve personel görevlerinin belirlenmesi konusundaki bulgular için gerekli mevzuat çalışmasının yapılıp yapılmadığı yazılı olarak istenmelidir. Konunun birim tarafından talimatlandırılmış veya bir mevzuata bağlanmış olmasına dikkat edilmesi gerekmektedir. Personel görevlerinin talimatlandırılmasının yanı sıra görevlendirilmiş personel ile konuşulmalı ve görevleri hakkında bilgisi olup olmadığı kontrol edilmelidir.

Mevzuat ile uygulama arasındaki farklardan doğan bulgularda, öncelikle uygulamadaki durumun mevzuata mı dönüştürüldüğü yoksa uygulamanın mevzuat hükümlerince yapılmasına mı karar verildiği bilgisi alınmalıdır. Mevzuat mevcut uygulamaya göre güncellenmiş ise doğruluğu kontrol edilmeli, uygulamanın mevzuata göre yapılacağı bilgisi alınmış ise personel mülakatı ve yerinde incelemeler ile durum kontrol edilmelidir. Veri tabanı yöneticileri ile yazılım geliştirme ekibinin ayrılması gibi görevler ayrılığı ilkesinin gerektirdiği durumlar kontrol edilmelidir. Birimler arası iletişim ile ilgili bulgular da bu kapsamda izlenerek iletişimin sağlıklı olup olmadığı ve hangi yollarla yapılmaya karar verildiği incelenmelidir. Seçilen yöntemlerin birimler arası iletişimde iyileşmeye yol açıp açmadığı belirlenmelidir.

Personel yetkinliği ve eğitimleri ile ilgili bulgularda, personel alım şartlarının değiştirilip değiştirilmediği, denetim sonrası istihdam edilen personelin yerleştirildiği pozisyona uygun olup olmadığı, eğitim ihtiyaçlarının tespit edilip planlamasının yapılıp yapılmadığının kontrol edilmesi gerekmektedir. İzleme sürecinden önce belirlenmiş konularda eğitim alınmışsa, eğitim ile ilgili dokümanlar incelenmeli, eğitim alan personelle görüşülüp eğitimin verimli olup olmadığı belirlenmelidir.

Olay yönetimi ile ilgili bulguların izlenmesinde olay anında yapılacakların yazılı hale getirilip getirilmediği, personelin olay anında yapması gerekenleri bilip bilmediği kontrol edilmelidir. Hazırlanan olay yönetim prosedürünün olası her durumu kapsayacak şekilde tasarlanmış olmasına dikkat edilmelidir. Daha önceki olay anlarının sebeplerinin ve alınan tedbirlerin kayıt altına alınıp alınmadığı, tekrar eden durumlarda yeni oluşturulan olay yönetim sürecinin etkin bir şekilde çözüm üretip üretmediği test edilmelidir.

Güncel envanter bilgisinin olmaması veya eksik olması ile ilgili bulgularda, envanter bilgisini tutmak için hangi yöntemin seçildiği tespit edilmelidir. Test amaçlı yeterli miktarda kayıt incelenmeli ve fiziksel olarak varlıkları tespit edilmelidir. Envanter kayıtlarının ne sıklıkla güncellendiği kontrol edilmelidir. Envanter bilgi sisteminin olmasının birime kattığı faydalar tespit edilmeli ve önemi vurgulanmalıdır.

Veri tabanı yönetimi ile ilgili birim haricinde başka birimlerce yönetilen veri tabanı olup olmadığı ile ilgili birimlerden bilgi istenip istenmediği, tespit edilmiş veri tabanlarının merkezi sisteme alınması ile ilgili çalışma ve ya planlama yapılıp yapılmadığı belirlenmelidir. Taşınamayacak veri tabanlarının neden taşınamayacağı ile ilgili sebepler incelenmelidir.

Veri tabanı standartlarının oluşturulmaması ile ilgili bulgular kritik öneme sahiptir. Standartların veri tabanı yönetiminin verimli ve etkin bir şekilde yürütülmesine zemin hazırlaması beklenir. Bu kapsamda oluşturulan standartlar incelenmeli bu standartların tüm kuruma tebliğ edilip edilmediği kontrol edilmelidir. Kurum içi bilgi teknolojileri projelerinde, veri tabanları için bu standartların kullanılması için yapılmış çalışmalar incelenmelidir.

3.4.2. Teknik Risklerin Oluşturduğu Bulguların İzlenmesi

Yedekleme ve bakım stratejileri ile ilgili bulgular izlenirken öncelikle konularla ilgili yazılı oluşturulmuş prosedürler incelenmelidir. Hangi aralıklarla ne tür yedekleme ve bakım yapılmasına karar verildiği incelenmeli ve mevcut durumla karşılaştırılmalıdır. Yedekleme ve bakım ile ilgili kullanılan veri tabanı yönetim sistemi yazılımında oluşturulmuş görevler incelenmeli, geçmişe yönelik hata kayıtları varsa sebepleri sorgulanmalıdır. Yedekten dönüş testlerinin yapıldığının kayıtları incelenmeli ve başarılı olduğu teyit edilmelidir.

Her zaman çevrim içi mimarisinin varlığı ve hangi veri tabanlarını kapsadığı izleme sırasında tespit edilmelidir. Her zaman çevrim içi mimarisi dışında kalan veri tabanlarının neden dışarıda bırakıldığı ile ilgili inceleme yapılmalıdır. Her zaman çevrim içi mimarisinde yük devretmenin (failover) hangi zamanlarda ve ne sebeple gerçekleştirildiği kayıtlarından incelenmeli ve bununla ilgili alınan önlemler sorgulanmalıdır. Rutin olarak yük devretme testlerinin yapılıp yapılmadığının kayıtları kontrol edilmelidir.

Veri değişim kayıtları (log) standartlarının oluşturulması izlenirken, log kayıtları içerisinde bulunması gereken veri tiplerinin neler olduğunun belirlenmiş olması ve bunun tüm yazılım geliştiricilere bildirilmiş olması kontrol edilmelidir. Standartların belirlenmesinden önce oluşturulmuş log kayıtlarının standart hale dönüştürülüp dönüştürülmediği, yeni veri tabanlarında ise log tablolarının standart halde olup olmadığı kontrol edilmelidir. Log kayıtları içinde arama yapıldığında ne sürede kayıtlara ulaşılabildiği test edilmeli, gerekli optimizasyon ve konsolidasyon işlemlerinin yapılıp yapılmadığı belirlenmelidir.

Denetim kayıtları (audit log) ile ilgili bulgular incelenirken kullanılan veri tabanı yönetim sistemi yazılımına göre sistem üzerinden hangi kayıtların açılmış olduğuna bakılmalıdır. Öneride belirlenen asgari denetim kayıt gruplarının varlığı kontrol edilmelidir. Hangi tarihten itibaren bu kayıtların tutulduğu ve olay görüntüleyicisi (event viewer) yardımıyla denetim kayıtlarının açıldığı tarihten itibaren kayıt almasını engelleyecek bir durum yaşanıp yaşanmadığı belirlemelidir.

Gerçek zamanlı izleme sisteminin incelenmesi iki başlık altında yapılmalıdır. Bunlardan ilki mesai saati içinde izleme, ikincisi ise mesai saati dışında izlemedir. Mesai saatleri içinde hangi yöntemle veri tabanlarını izledikleri belirlenmelidir. İzleme monitörlerinin varlığı, hangi kaynakları izledikleri (bellek, işlemci, depolama) ve olası bir olayı bu izleme sistemiyle tespit edip edemeyecekleri belirlenmelidir. Mesai dışı saatlerde uyarı sisteminin varlığı kontrol edilmelidir. SMS veya e posta gibi teknolojilerle oluşturulan uyarı sistemiyle olay anında müdahale edilip edilmediği ve mesai harici olan olaylara müdahale için personel belirlenip belirlenmediği incelenmelidir.

Kullanıcı erişim ve yetkilendirme ile ilgili bulgularda öncelikle veri tabanı yönetim sistemi uygulamalarında bulunan yönetici (admin) yetkili kullanıcılar tespit edilmelidir. Bu kullanıcıların gerçekten veri tabanı yöneticisi olduğu, kullanıcı adlarının tekil olduğu, ortak bir kullanıcı kullanarak sisteme yönetici olarak bağlanmadıkları belirlenmelidir. Sistem içinde varsayılan olarak tanımlı "sa", "postgres" gibi yönetici yetkili kullanıcıların pasif durumda olup olmadıkları kontrol edilmeli, parola karmaşıklık ve geçerlilik süreleri ile ilgili tanımlı kurallar incelenmeli, istisnai kullanıcı olup olmadığı belirlenmelidir. Uygulama kullanıcılarına ve kişisel kullanıcılara yetki verilmesi ve kullanıcı açılması ile ilgili prosedürlerin varlığı sorgulanmalı ve taleplerin kayıt altında tutulduğu belirlenmelidir.

Canlı, test ve geliştirme ortamları ile ilgili bulguların izlenmesine öncelikle tüm ortamların mevcut olup olmadığının kontrolü ile başlanmalıdır. Kaynak yetersizliği veya risk eşiğinin düşüklüğü gibi sebeplerden bazen geliştirme ve test ortamı birleştirilebilmektedir. Test ve geliştirme ortamındaki veriler incelenmeli, gerçek veri olup olmadığı kontrol edilmelidir. Canlı ve test ortamlarındaki kullanıcı yetkileri ayrı ayrı incelenmelidir. Canlı ortamda uygulama kullanıcısından başka yetkili kullanıcı olmadığı tespiti yapılmalıdır. Canlı ortamda yönetici yetkisine sahip uygulama kullanıcısı olup olmadığının kontrol edilmesi önemli görülmektedir.

4. SONUÇ VE ÖNERİLER

Kamu idarelerinde elektronik ortamdan kesintisiz olarak sunulan hizmetlerin sayısı gün geçtikçe artmakta olup, bu hizmetlerin devamlılığının ve güvenliğinin sağlanması da aynı şekilde önem kazanmaktadır. Bilgilerin elde edildiği veriler, veri tabanı yönetim

sistemleri araçlarıyla yönetilmektedir. Veri tabanı yönetim sistemleri büyük çaplı verileri saklama, değiştirme ve koruma gibi süreçleri kolaylaştırmaktadır. Bilgi teknolojileri denetim süreçlerinden biri olan veri tabanı yönetimi denetimi; standart veri tabanı yönetiminin hayata geçirilmesi, ilgili mevzuatlara, talimatlara, politika ve prosedürlere göre uygun hizmet verilmesinin sağlanması, varsa süreçte aksayan yönlerin geliştirilerek yürütülen çalışmalara değer katma prensibi amacıyla belirli periyotlarla gerçekleştirilmelidir. İç denetçiler veri tabanı yönetimi denetiminde idari riskleri belirlemede zorluk yaşamamasına rağmen teknik riskleri belirlemede zorluklar yaşayabilmektedir. Denetimlerin başarıyla sonuçlandırılabilmesi bakımından, denetim ekibi oluşturulurken bu husus göz önünde bulundurulmalıdır.

Denetim ile birlikte veri tabanları yönetiminin teknik ve idari kontrollerini geliştirmek için önemli öneriler ortaya çıkacaktır. Önerilerin gerçekleştirme tarihleri bulgunun risk seviyesi ve denetlenen birimin kaynak durumuna göre belirlenmelidir. Özellikle risk seviyesi yüksek teknik bulgular ile ilgili önerilerin gerçekleştirilme zamanı mümkün olduğunca kısa tutulmalı ve sonuçları yerinde incelenmelidir.

Denetim sürecinin aktörleri denetçiler, denetlenenler ve üst yönetimdir. Denetiminin istenilen makul güvenceyi sağlayabilmesi için tüm aktörlerin sürece katkı sağlaması gerekmektedir. Veri tabanı yönetimi uzmanlık gerektiren bir iş olduğundan, denetim ekibi içinde mutlaka teknik konudan anlayan bir denetçinin veya destek alınan bir dış uzmanın olması başarıyı artıracaktır. Denetlenen taraf denetimin, süreci iyileştirmek için yapıldığının farkında olmalı, denetim ekibi tarafından oluşturulan bulgular ve bu bulguların önerilerini makul sürede gerçekleştirmelidir. Üst yönetimin desteğini almak hem denetçiler hem de denetlenenler tarafından önemlidir. Denetçiler mevcut durumu, olması gereken durumu, bulguları ve önerileri üst yönetime aktarmalı ve farkındalık yaratmalıdır. Denetlenen taraf ise önerilerin gerçekleştirilmesi için uygulayacakları eylemleri üst yönetime doğru ve eksiksiz anlatmalı ve desteğini almalıdır.

Yönetimin onayı ile önerilerin uygulanması ve sürdürülmesi büyük önem arz etmektedir. Denetim sonucunda yasalara uyum, verinin korunması, standartların oluşturulması, yetkin personel istihdamı, sistem sürekliliği, kesintisiz hizmet sunulması, kaynakların etkin ve verimli kullanılması hususlarına ilişkin makul güvence sağlanmış olacaktır.

Kaynakça

De Haes, S., & Van Grembergen, W. (2006). Information Technology Governance Best Practices in Belgian Organisations. Proceedings of the 39th Annual Hawaii International Conference on System Sciences (HICSS'06). doi:10.1109/hicss.2006.222.

Henkoğlu T.,Yılmaz, B. (2013). Avrupa Birliği (AB) Bilgi Güvenliği Politikaları. *Türk Kütüphaneciliği 27, 3 (2013)*, 451-471. Erişim adresi: http://www.bby.hacettepe.edu.tr/e-bulten/dosyalar/file/Eylul2013/henkoglu_yilmaz_tk.pdf.

Koçel T., (1982). *İşletme Yöneticiliği,* İstanbul: Beta Yayınları.

Köklü K. (2018). İşAnalizi, İş Analistliği ve İş Zekası. *Lectio Socialis*, *Volume 2, Issue 2*, 121-142 Erişim Adresi: http://dergipark.gov.tr/download/article-file/515874.

McCumber, J. (2005). *Assessing and managing security risk in IT systems.* Washington: CRC.

Muradova T. (2007). İnsan Kaynakları Yönetiminde Eğitim ve Geliştirmenin Önemi, *Khazar Journal Of Azerbaijani Studies, 10*(3-4), 75–84. Erişim Adresi :http://www.jhss-khazar.org/2009-12-2/INSAN%20KAYNAKLARI%20YONETIMINDE%20EGITIM%20VE%20GELISTIRMENIN%20ONEMI.pdf.

Oz E. (2008). *Management Information Systems* (6. bs.). Course Technology.

Prabhjot P., Sharma N. (2017). Overview of the Database Management System. *International Journal of Advanced Research in Computer Science,* Vol 8, No 4. Erişim adresi: http://www.ijarcs.info/index.php/Ijarcs/article/download/3778/3259.

Ramakrishnan R., Gehrke J. (2003). *Database Management Systems* (3. bs.). McGraw-Hill Education.

Sevim, A. (2005). "Veri Tabanı ve Yönetimi". *Muhasebe Bilgi Sistemi.* Ed. F. Sürmeli. Eskişehir: Açık Öğretim Fakültesi Yayınları no.860. 82-83.

Sevinç, İ. (2007). Kamu Kurumlarında Bilgi Teknolojileri Kullanımı Ve Bunların Çalışanların Fiziksel Ve Psikolojik Durumlarına Etkileri. *Journal of Knowledge Economy & Knowledge Management 2007,* (Volume II Spring), 21-31. Erişim Adresi:http://beykon.org/dergi/2007/I.Sevinc.doc.

İç Denetim Koordinasyon Kurulu. (2014). *Kamu Bilgi TeknolojileriDenetimiRehberi* (1. sürüm). Erişim adresi: http://www.idkk.gov.tr/SiteDokumanlari/Mevzuat/Ucuncul%20Duzey%20Mevzuat/KamuBTDenetimiRehberi/KamuBTDenetimiRehberi.pdf.

İç Denetim Koordinasyon Kurulu. (2014). *Kamu* İç *Denetim Rehberi* (1. sürüm). Erişim adresi: http://www.idkk.gov.tr/SiteDokumanlari/Mevzuat/Ucuncul%20Duzey%20Mevzuat/K%C4%B0DR_v1.0.pdf.

Kamu İç Kontrol Standartları Tebliği. (2007, 26 Aralık). *Resmi-Gazete (Sayı:26738).* Erişim adresi: http://www.resmigazete.gov.tr/eskiler/2007/12/20071226-21.htm.

TS ISO/IEC 27001:2013, Bilgi teknolojisi - Güvenlik teknikleri - Bilgi güvenliği yönetim sistemleri - Gereksinimler.

Types of database management system and their evolution. (2014, 24 Kasım). Erişim adresi: https://www.analyticsvidhya.com/blog/2014/11/types-databases-evolution/.

Veritabanı. (2018). ISACA terimler sözlüğünde. Erişim adresi: https://www.isaca.org/About-ISACA/History/Documents/ISACA-Glossary-English-Turkish_mis_Tur_0418.pdf.

İnternet Kaynakları

Bilgi. (t.y.). Türk Dil Kurumu Türkçe Sözlük. Erişim adresi: http://www.tdk.gov.tr/index.php? option=com_gts&view=gts (Erişim Tarihi:20 Aralık 2018).

NoSQL Nedir?. (t.y.). Erişim adresi: https://aws.amazon.com/tr/nosql/ (Erişim Tarihi:09 Ocak 2019).

Oracle (2019), Database Auditing: Security Considerations. Erişim adresi: https://docs.oracle.com/cd/B19306_01/network.102/b14266/auditing.htm#CHDJBDHJ (Erişim Tarihi: 01 Şubat 2019).

SimpliLearn. (2019, Nisan). Introduction to NoSQL databases Tutorial. Erişim adresi: https://www.simplilearn.com/introduction-to-nosql-databases-tutorial-video (Erişim Tarihi:03 Nisan 2019).

Standards and procedures for database systems. (t.y.). Erişim adresi:https://www.ibm.com/support/knowledgecenter/en/SSEPH2_15.1.0/com.ibm.ims15.doc.dag/ims_dbsystemstds.htm (Erişim Tarihi: 02 Nisan 2019).

Unipedi (2014, Ocak).İlişkisel Veritabanı. Erişim adresi:http://www.unipedi.com/teknoloji/tag/iliskisel-veritabani-ozellikleri/ (Erişim Tarihi:04 Ocak 2019).

What is a Relational Database Management System?. (t.y.). Erişim adresi: https://www.codecademy.com/articles/what-is-rdbms-sql (Erişim Tarihi:21 Ocak 2019).