BANKACILIK
DÜZENLEME VE DENETLEME
KURUMU

BDDK Çalışma Raporları : 2006-2

Operasyonel Risk Veri Tabanı Modellemesi

Mart - 2006

BANKACILIK DÜZENLEME VE DENETLEME KURUMU

BDDK Çalışma Raporları No: 2006/2

Operasyonel Risk Veri Tabanı Modellemesi

Murat MAZIBAŞ*

* *Bankacılık Uzmanı, Strateji Geliştirme Dairesi, Bankacılık Düzenleme ve Denetleme Kurumu (BDDK)*

Bu çalışmada yer verilen görüşler yazarın sorumluluğunda olup Bankacılık Düzenleme ve Denetleme Kurumunu bağlamaz.

Bilgi ve Görüşleriniz İçin:
Murat MAZIBAŞ (312) 455 6641, mmazibas@bddk.org.tr

Operational Risk Database Modelling

ABSTRACT

For operational risk management, existence of qualified and analytically tractable data, and collection of this data into a systematic database is a mandate. An important phase in studies on developing an operational risk management system is construction of an operational risk database.

In the development process of an operational risk database, the most fundamental parts are defining the risk data and designing the architecture of the database. Defining the risk data requires careful analysis of risks that bank is exposed to. This process begins with a comprehensive search for elements and sources of risks. In this process the most fundamental question to be answered is what is operational risk and operational loss. Another central task is defining the basic properties and qualities of data, determining the data needs of measurement methodologies, identifying types and sources of data.

For an operational risk database, a proper foundation is crucial to ensure that the structure is built to last. Therefore, each step in the construction has to be handled with care. In this manner, in order to begin with a proper foundation, planning and preparation has to be comprehensive. Designing a database architecture best fitting the bank's needs is crucial. Thereof conceptual, logical and physical design phases are immensely important. Implementation phase is the phase where actual performance of the database is tested.

Through giving essential information on operational risk data and database modelling, main aim of this paper is to contribute to the banks' efforts on this topic. In this manner, this paper is organized for providing the most essential and if necessary detailed technical knowledge on developing an operational risk loss database. In the first part, it is discussed that what are the fundamental properties of operational risk data to be eligible for inclusion into the database, what are the data types and data requirements of Basel-II operational risk advanced measurement approaches, and how and from where shall these data be obtained. In the second part, basic information about the building of a database (database, database modeling, database system etc.) is given. Third part is devoted to the development of an operational risk database and in this part; stages of planning, conceptual design, logical design, physical design and implementation are discussed.

Operasyonel Risk Veri Tabanı Modellemesi

ÖZET

Operasyonel risklerin yönetilebilmesi için nitelikli ve analize uygun verilerin mevcut olması ve bu verilerin sistematik bir veri tabanında toplanması önemli bir ön koşuldur. Operasyonel risk yönetim sisteminin kurulmasına yönelik çalışmalardaki en önemli aşamalardan birisi de operasyonel risk veri tabanının oluşturulmasıdır.

Operasyonel risk veri tabanının oluşturulması sürecindeki en temel bölüm riskin tanımlanması ve veri tabanı mimarisinin tasarlanmasıdır. Risk verilerinin belirlenmesi, bankanın maruz bulunduğu risklerin dikkatli bir şekilde analiz edilmesini gerektirmektedir. Bu süreç, risk etkenlerinin ve kaynaklarının kapsamlı taraması ile başlamaktadır. Bu süreçte, cevaplandırılması gereken en temel soru operasyonel riskin ve operasyonel kayıp olayının ne olduğudur. Bir diğer önemli görev ise risk verilerinin sahip olması gereken temel özelliklerin tanımlanması, ölçüm yöntemleri için gerekli risk verilerinin ve bu verilerin elde edileceği kaynakların belirlenmesidir.

Operasyonel risk veri tabanının doğru ve uygun bir temel üzerine inşası, veri tabanının uzun yıllar amaca hizmet edebilmesi için önemlidir. Tüm çalışmaların ve veri tabanının doğru ve uygun temel üzerine bina edilebilmesi için planlama ve ön hazırlık aşamaları kapsamlı bir şekilde ele alınmalıdır. Bankanın ihtiyaçlarına en uygun veri tabanının tasarımını gerçekleştirmek önemlidir. Bu çerçevede, kavramsal, mantıksal ve fiziksel tasarım süreçleri çok önemli hale gelmektedir. Uygulama süreci, veri tabanının gerçek performansının test edilme ve varsa gerekli düzeltmelerin yapılmasına imkân sağlayan bir süreçtir.

Çalışmanın temel amacı, risk verilerine ve veri tabanı modellemesine ilişkin temel bilgileri aktarmak suretiyle bankaların bu konudaki çalışmalarına katkıda bulunmaktır. Çalışma, operasyonel risk veri tabanı sisteminin oluşturulması esnasında gerekli asgari düzeydeki bilgilerin aktarımına yönelik olarak bölümlere ayrılmıştır. Bu amaçla, ilk bölümde, operasyonel risk verilerinin sahip olması gereken temel özelliklerin neler olduğu, Basel-II' de yer alan ileri ölçüm yöntemleri ile bunlar için gerekli veriler, operasyonel risk veri çeşitlerinin neler olduğu ve bunların nerelerden elde edilebileceği konuları ele alınmıştır. İkinci bölümde, veri tabanı modellemesine ilişkin temel bilgilerin verilmesi amacıyla veri tabanı modellemesi, veri modellemesi, veri tabanı tasarımı gibi temel kavramlarla birlikte veri tabanı sisteminin işleyiş yapısı ve oluşturulma süreci konuları ele alınmıştır. Üçüncü bölümde, operasyonel risk veri tabanının oluşturulması süreci planlama, kavramsal tasarım, mantıksal tasarım, fiziksel tasarım ve uygulamadan oluşan beş aşamada ele alınmıştır.

İÇİNDEKİLER

TABLO VE ŞEKİLLER

KISALTMALAR

BBA	İngiliz Bankacılar Birliği (British Bankers Association)
BCBS	Basel Komitesi (Basel Committee on Banking Supervision)
CP2	İkinci İstişare Metni (Consultative Paper 2)
DDL	Veri Tanımlama Dili (data definition language)
DML	Veri İşleme Dili (data-manipulation language)
ER	Varlık-İlişki yaklaşımı (Entity-Relationship Approach)
fk	Yabancı Anahtar (Foreign Key)
GA	Gereksinim Analizi
İÖY	İçsel Ölçüm Yaklaşımı (Internal Measurement Approach)
KDY	Kayıp Dağılımları Yaklaşımı (Loss Distribution Approach)
QL	Sorgu Dili (Query Language)
pk	Temel Anahtar (Primary Key)
RMD	Riske Maruz Değer (Value at Risk)
SKY	Skor Kart Yaklaşımı (Scorecard Approach)
VTYS	Veri Tabanı Yönetimi Sistemi

GİRİŞ

Yeni Basel Sermaye Uzlaşısı (Basel-II) operasyonel riskler konusundaki farkındalığın gelişimine önemli katkılarda bulunmaktadır[1]. Operasyonel risklerin de yasal sermaye tahsis edilmesi gereken riskler arasına dahil edilmesi ile operasyonel riskin mutlaka yönetilmesi gereken önemli bir risk olduğu konusundaki bilinç pekişmiştir. Operasyonel riskin niteliği ile potansiyel etkileri ve bu etkilerin boyutu, riskin anlaşılabilmesi için mutlaka sayısallaştırılmasını ve ölçülmesini gerektirmektedir.

Risklerin ölçümü ve yönetimi sürecinin temel unsurlarından birisi de riskle ilgili verilerdir. Her türlü riskin ölçülebilmesi ve yönetilebilmesi için risk verilerinin mevcut olması öncelikli koşuldur.

Niteliği gereği operasyonel risk, finansal riskler ile diğer finansal olmayan risklerden belirgin farklılıklar taşımaktadır. Operasyonel riskin bankanın faaliyetlerindeki sistem, süreç ve insan unsurları ile yönetimin kontrolü altında bulunmayan dışsal etkenler nedeniyle ortaya çıkması riskin kapsamını da genişletmektedir.

Operasyonel riskin kendine özgü özellikleri ve kapsamının genişliği, riskin ölçülebilmesi ve yönetilebilmesi için oldukça geniş kapsamlı ve çok çeşitli verilerin toplanmasını zorunlu kılmaktadır. Bankanın operasyonel risk veri tabanına aktarılacak verilerin kalitesi risk ölçümünün ve yönetiminin başarısını da belirleyen önemli etkenlerin başında gelmektedir. Risk ölçümü, verinin mevcudiyeti halinde mümkündür ve risk yönetimi de yeterli düzeyde bilgilendirme halinde yapılabilmektedir. Verilerin gerekli nitelikleri taşımaması, risk ölçümlerinin de sapmalı veya hatalı olmasına neden olabilmektedir. Gerçekleştirilen risk yönetimi faaliyetlerinin, yanlış veya eksik bilgilendirmeye dayanmasına neden olabilecek böyle bir durumun kendisi ciddi bir operasyonel risk ortaya çıkarmaktadır.

Risk verilerinin toplanması ve bunların analize uygun hale getirilmesi için bir veri tabanı sisteminin bulunması gereklidir. Operasyonel risk veri tabanı, tüm iş kollarından ve faaliyetlerinden, birbirinden farklı birçok operasyonel risk verisi topluyor olması nedeniyle kapsamı ve sürece katılan birimler itibariyle bir bankanın en kapsamlı veri tabanı sistemlerinden birisini oluşturmalıdır. Veri tabanının kapsamının geniş olması, oluşturulması sürecinin de buna göre şekillendirilmesini gerektirmektedir.

[1] Basel Komitesinin operasyonel riske yaklaşımına ve Basel-II'de operasyonel riskin ele alınışına ilişkin bir değerlendirme için bakınız: Mazıbaş (2005c).

Bu çalışmanın temel amaçlarından ilki, operasyonel risklerin ölçümü için gerekli olan operasyonel risk veri tabanının ne olduğu ve nasıl oluşturulabileceği konularında kapsamlı ve detaylı bilgiler aktarmak suretiyle bu konuda çalışma yürüten veya yürütmeyi planlayan bankaların çalışmalarına katkıda bulunmaktır. Bir diğer amacı ise, operasyonel risklerin ölçülebilmesi ve yönetilebilmesinin ilk koşulu olan risk hakkında bilgi sahibi olunmasını sağlayabilmek amacıyla risk verileri konusundaki bilincin geliştirilmesine katkıda bulunmaktır.

Bu amaçlar çerçevesinde, birinci bölümde operasyonel risk verileri konusunda temel bilgilerin aktarılabilmesi için verilerin sahip olması gereken temel özellikler, ölçüm yaklaşımları itibariyle risk verileri, veri çeşitleri ve veri kaynakları konuları ele alınmaktadır.

İkinci bölümde, veri ve veri tabanı modellemesine yönelik temel bilgileri aktarmak amacıyla veri tabanı modellemesi, veri modellemesi, veri tabanı tasarımı, veri tabanı sisteminin temel işleyiş yapısı ve veri tabanının oluşturulması süreçlerinden oluşan temel konulara yer verilmektedir.

Üçüncü bölümde ise, bir bankada operasyonel risk veri tabanı sisteminin kurulması aşamalar itibariyle ele alınarak her aşamada yapılması gerekenlere yer verilmektedir.

I. OPERASYONEL RİSK VERİLERİ

Verinin mevcudiyeti, her türlü riskin ölçümü ve yönetimi için gereklidir. Operasyonel risk hakkında bilgi edinebilmek için riskin kendisini gösterdiği olay, bu risk olayının ortaya çıkmasına neden olan etkenlerle koşullar ve olay nedeniyle karşı karşıya kalınan kayıplar hakkında yeterli bilginin mevcut olması gereklidir. Bunların yanında doğrudan operasyonel risk hakkında bilgi vermese de dolaylı olarak riskin gelişimiyle ilgili bilgi sağlayan çeşitli risk göstergeleri hakkında bilgiler de gereklidir[2]. Operasyonel risk ölçüm süreci, ölçümün amacı ve kapsamı ile kullanılan yönteme bağlı olarak farklı veri gereksinimleri ortaya çıkarmaktadır.

Basel Bankacılık Denetim Komitesinin (Komite) operasyonel risk verilerine yaklaşımı, ileri ölçüm yöntemlerinde kullanılan verilere standartlar getirmek ve standart veri sınıflandırmaları ile iş kolu ve faaliyet sınıflandırmaları geliştirilmesinden oluşmaktadır[3].

Komite, bankaların ileri ölçüm yaklaşımları kapsamında asgari olarak kullanacakları verileri; içsel veriler, dışsal veriler, senaryo analizleri ve iş koşulları ile kontrol ortamına ait bilgiler olmak üzere dört grupta ele almaktadır. Komite, bu verilerin niteliğine ve yasal sermaye yükümlülüğünün hesaplanmasında kullanımına dair asgari standartları belirlemektedir.

Komite, operasyonel risk verilerini nedensellik ve kayıp verileri olmak üzere iki ana grupta ele alarak kayıp verilerine ait detaylı sınıflandırmayı belirlemiştir. Ayrıca, bankalar için sekiz ana iş kolu belirlemiştir. Bankaların yasal sermaye yükümlülüklerinin hesaplanmasında bu sınıflandırmaya uygun hareket etmeleri ve denetim otoritelerinin de bankaların bu sınıflandırmaya uyum düzeyini değerlendirmesi gerekmektedir.

Bu bölümde, operasyonel risk verileriyle ilgili olarak gerek Basel Komitesi tarafından belirlenen standartlar gerekse de uluslararası bankacılık sistemindeki en iyi uygulamalar göz önünde bulundurularak, operasyonel risk verilerinin sahip olması gereken temel özelliklerin neler olduğu, Basel-II'de yer alan ileri ölçüm yöntemleri ile bunlar için gerekli veriler, operasyonel risk veri çeşitlerinin neler olduğu ve bunların nerelerden elde edilebileceği konuları ele alınmaktadır.

[2] İçsel kayıp verileri ile skor kart ve senaryo analizi verilerinin bir arada ele alınmasına yönelik olarak bakınız Fujii (2003).

[3] Basel Komitesinin operasyonel risk verilerine yaklaşımına yönelik bir değerlendirme için bakınız Mazıbaş (2005b).

A. Verilerin Sahip Olması Gereken Temel Özellikler

Operasyonel risk verilerinin risk ölçümü ve yönetimi sürecinde kullanılabilmesi için bir takım temel özelliklere sahip olmaları gerekmektedir. Bu temel özellikler şunlardan oluşmalıdır:

- Doğru olma
- Tam olma (eksiksizlik)
- Zamanında erişilebilir olma
- Tutarlı olma
- Detaylılık (granularity)
- İncelemeye elverişli olma

1-Doğruluk: Operasyonel risk verileri operasyonel risk olayları, kayıplar ve olayların nedenleri konusunda doğru bilgiler aktarmalıdır. Veriler, kullanıcılar veya veriyi hazırlayanlar tarafından, dayandığı olay veya oluşumla ilgili olarak gerçeğinden farklı bilgiler aktarmasına neden olabilecek şekilde değiştirilmemiş olmalıdır.

2-Tamlık (Eksiksizlik): Operasyonel risk verileri, hakkında bilgi aktardığı konu, olay veya oluşumla ilgili olarak ihtiyaç duyulan kapsam ve nitelikte eksiksiz bilgi aktarabilmelidir.

3-Zamanında Erişilebilirlik: Operasyonel risk verileri kullanım amaçlarına göre uygun zamanda mevcut olmalıdır. Veriler analiz için gerekli zamanda hazır, amaca uygun zaman boyutunu kapsar nitelikte ve istenildiği anda ulaşılabilir olmalıdır.

4-Tutarlılık: Operasyonel risk verileri kendi içerisinde ve benzer diğer verilerle tutarlı olmalıdır. Verilerin kendi içerisinde çelişkiler taşımaması, bütünlüğünün bulunması, aynı konu, olay veya oluşuma ait farklı kaynaklardan elde edilen benzer verilerle çelişkiler taşımaması analizin sağlığı açısından gereklidir.

5-Detaylılık: Operasyonel risk verileri bir konu, olay veya oluşum hakkında bütüncül verilerin yanında istenilen detay düzeyinde de bilgiler içerebilmelidir. Kayıp ve nedensellik verileri her bir olay bazında ele alınabilir olmalı ve risk olayı hakkında gereken düzeyde detaylı bilgi içeriyor olmalıdır.

6-İncelemeye Elverişlilik: Operasyonel risk verileri, bankanın iç ve dış denetçileri tarafından kontrol edilebilir ve incelenebilir olmalıdır. Verilerin kontrole ve denetime uygun formatta, kapsamda ve nitelikte olması risk ölçümü ve yönetimi sürecinin kontrolünün ve denetiminin gereğince yapılabilmesi için gereklidir.

B. Operasyonel Risk Verileri ve Ölçüm Yöntemleri

Operasyonel riskin ölçülebilmesinin öncelikli koşulu risk olaylarına ait verilerin mevcudiyetidir. Operasyonel riskin güvenilir bir şekilde ölçülebilmesi için öncelikli olarak bankanın risk profilini yansıtan içsel verilerin toplanması gereklidir. Bunun yanında henüz tecrübe edilmemiş ancak benzer özelliklere sahip diğer bankaların tecrübe ettiği kayıp olaylarına ait dışsal verilerin de toplanması gereklidir. İçsel ve dışsal verilerden oluşan güvenilir bir veri tabanının oluşturulması önemli bir adımdır. Oluşturulan veri tabanı benimsenen risk ölçüm yaklaşımında kullanılacak verilerin yanında geliştirilmekte olan veya geliştirilmesi planlanan yöntemlerin de ihtiyacını karşılayabilecek verileri içerebilmelidir.

Basel Komitesi, (BCBS, 1998)'de operasyonel risk yönetiminin önemini belirterek, kredi ve piyasa riskinin yanında operasyonel riskler için de yasal sermaye yükümlülüğü getirilebileceğinin ilk sinyallerini vermiştir. Komite, İkinci İstişare Metni-CP2 (BCBS, 2001b) ile yasal sermaye yükümlülüğüne dahil ettiği operasyonel riskler için sermayenin hesaplanmasında kullanılacak yöntemlere (BCBS, 2001a)'da yer vermiştir. (BCBS, 2001c)'de basit yöntemler olan Temel Gösterge Yaklaşımı ve Standart Yaklaşımın yanında, Kayıp Dağılımları Yaklaşımı gibi ileri yöntemlere geçişte kullanılabilecek İçsel Ölçüm Yaklaşımı detaylı bir şekilde ele alınmıştır. Ancak, Komite, ileri ölçüm yaklaşımlarına ilişkin olarak belirli bazı modellere yer verilmesinin bu konudaki gelişmelere engel olacağı düşüncesinden hareketle Üçüncü İstişare Metninde-CP3 (BCBS, 2003) ve nihai Basel II metninde (BCBS, 2004 ve 2005) herhangi bir model ismine yer vermemiştir.

Ancak, halen bankacılık sektöründe operasyonel riskler için yasal sermaye yükümlülüğünün hesaplanmasında ileri ölçüm yöntemleri ile bu yöntemlere geçişte kullanılabilecek, şimdilik, üç farklı ölçüm yaklaşımı bulunmaktadır:

- İçsel Ölçüm Yaklaşımı (İÖY)
- Kayıp Dağılımları Yaklaşımı (KDY)
- Skor Kart Yaklaşımı (SKY)

1. İçsel Ölçüm Yaklaşımı (İÖY)

Komitenin operasyonel riskleri de yasal sermaye yükümlülüğü kapsamına dahil ettiği CP2'de, ileri ölçüm yöntemlerine geçişte kullanılabilecek ara bir yöntem olarak İçsel Ölçüm Yaklaşımına (İÖY) yer verilmiştir.

İÖY yaklaşımında, hesaplama yöntemi denetim otoritesi tarafından tüm bankalar için standart olarak belirlenmekle birlikte, bankalara kendi kayıp verilerini kullanma imkânı verilmektedir. Denetim otoriteleri, bu yaklaşımın kullanılabilmesi için bankaların ölçüm

yaklaşımının doğruluğu, veri kalitesi ve iç kontrol ortamının yeterliliği konusunda nicel ve nitel bazı standartlara uyum sağlamalarını istemektedir. Komite, İÖY yaklaşımının bankaları içsel kayıp verisini toplamaya teşvik etmek suretiyle daha gelişmiş yaklaşımlara geçişte kritik bir adım olduğuna inanmaktadır (BCBS, 2001a).

Komite tarafından, bu yaklaşım kapsamında yasal sermayenin hesaplanma aşamaları şu şekilde ifade edilmektedir (BCBS, 2001b):

- Banka faaliyetleri standart yaklaşımda da kullanılan iş kollarına ayrılarak, operasyonel risk türleri geniş bir şekilde tanımlanır ve tüm iş kolları için uygulanır.
- Denetim otoritesi tarafından her bir iş kolu/risk türü birleşimi için iş kolunda maruz bulunulan operasyonel riskin büyüklüğü (veya miktarı) hakkında bilgi veren bir risk tutarı göstergesi (brüt gelir, işlem adedi gibi) belirlenir.
- Her bir iş kolu/risk türü birleşimi için, risk tutarı göstergesinin yanında banka tarafından içsel kayıp verilerinden yararlanılarak kayıp olayının gerçekleşme olasılığı ve kayıp olayı gerçekleştiğinde ortaya çıkabilecek kayıp tutarına ilişkin parametreler belirlenir. Belirlenen risk tutarı göstergesi, kayıp olayı olasılığı ve kayıp tutarı kullanılarak beklenen kayıp miktarı hesaplanır.
- Denetim otoritesi tarafından, beklenen kaybı beklenmeyen kayba dönüştürmekte kullanılacak olan ve sektör geneline ait veriler kullanılarak her bir iş kolu/risk türü birleşimi için "gamma" olarak adlandırılan bir faktör belirlenir. Sermaye tutarı, beklenen kayıp ve gamma faktörleri kullanılarak hesaplanır.
- Bankanın tamamı için hesaplanacak sermaye miktarı, her bir iş kolu/risk türü birleşimi için hesaplanan sermaye tutarlarının basit toplamından oluşmaktadır.

İÖY yaklaşımı için gerekli veriler, bankanın her bir iş kolu/risk türü birleşimi için kayıp verilerinden yararlanılarak belirlenen kayıp olayı olasılığı ve kayıp olayı halinde ortaya çıkan kayıp miktarına ilişkin parametreler ile risk tutarı göstergelerine ait bilgiler ve denetim otoritesi tarafından belirlenen "gamma" faktörlerinden oluşmaktadır.

2. Kayıp Dağılımları Yaklaşımı (KDY)

Komite, aktüeryal matematik modellere dayanan ve kayıp dağılımlarından risk ölçütü olarak Operasyonel Riske Maruz Değer (RMD) tutarına ulaşılan Kayıp Dağılımları Yaklaşımlarına (KDY) ilk olarak BCBS (2001a)'da yer vermiştir.

Bu yaklaşımda, iş kolları/kayıp olayları matrisindeki her bir hücre veya hücre gruplarının gelecek dönemdeki (bir yıl gibi) olası operasyonel risk kayıp dağılımı

hesaplanmaktadır. Bu hesaplamalar sonucu bulunan sermaye gereksinimi, kayıp dağılımının yüksek bir yüzdelik dilimindeki tutarına dayanmaktadır. Kullanılan kayıp dağılımı, İÖY'de olduğu gibi, operasyonel risk kayıp olayının sıklığı ve büyüklüğüyle ilgili varsayımlara dayalı olarak üretilmektedir. KDY, özellikle, operasyonel risk kayıp olaylarının sıklığına ve her bir olayın büyüklüğüne ilişkin dağılımların şeklinin hesaplanmasını içermektedir. Bu hesaplamalar, spesifik dağılım varsayımlarının empoze edilmesini veya Boot-Strapping ve Monte Carlo Simülasyonu gibi teknikler kullanılarak dağılımların ampirik olarak türetilmesini içerebilmektedir. Toplam sermaye yükümlülüğü, her bir iş kolu / kayıp olayı türü birleşimi için hesaplanan operasyonel risk tutarlarının basit toplamına ya da korelasyonun riskleri azaltıcı etkisini dikkate alan diğer toplama yöntemlerinin kullanımına dayanmaktadır[4].

KDY için gerekli veriler bankanın her bir iş kolu ve faaliyet alanındaki kayıp olaylarına ait sıklık ve büyüklük verilerinden oluşmaktadır.

3. Skor Kart Yaklaşımı (SKY)

Bu yaklaşım, her bir iş kolu ve risk sınıfı için operasyonel kayıpların ortaya çıkmasına neden olan ana etkenlerin tanımlanması ve bu etkenlere öncelik verilmesi suretiyle yasal sermayenin doğrudan hesaplanması sürecine ileri bakışlılık özelliği kazandırmak amacıyla geliştirilmiş bir sermaye hesaplama yaklaşımıdır.

Bu yaklaşımda tahsis edilen sermayenin seviyesi, risklerle ilgili kontrollerin varlığı ve etkililiği konusunda yapılan değerlendirmeye dayanmaktadır. Bu değerlendirmeler, derecelendirme amaçlı olarak sorulan sorulara verilen cevaplardan elde edilmektedir. Ardından, skor kart sorularına verilen cevaplar asgari yasal sermaye yeterliliğinin belirlenmesi için uygun bir şekilde ağırlıklandırılan her bir iş kolu ve risk sınıfı birleşimi için risk derecelerinin belirlenmesinde kullanılmaktadır. Bu şekilde bir yöntemin benimsenmesi riske duyarlı sermaye tahsisiyle birlikte gerekli iş kollarında kontrollerin güçlendirilmesi için gerekli teşvikleri de sağlamaktadır.

Skor kart yaklaşımı için gerekli verilerden başlıcaları kayıp verisi ile birlikte her bir iş kolu-risk türü için belirlenen risk göstergesine ait verilerden oluşmaktadır.

C. Veri Çeşitleri

Operasyonel riskin ölçümü süreci, ölçümün amacı ve kapsamı ile kullanılan yönteme bağlı olarak farklı veri gereksinimlerini ortaya çıkarmaktadır.

[4] Kayıp Dağılımı Yaklaşımına ilişkin Basel Komitesinin Yaklaşımı için bakınız BCBS (2001a). KDY yaklaşımının teorik temeli, KDY kullanılarak yapılan ölçüme ve sermaye tahsisine ilişkin uygulamalar için bakınız Mazıbaş (2002), (2005a), (2005b), (2005e).

Operasyonel risklerin ölçümü ve yönetimi sürecinde ihtiyaç duyulan verileri başlıca altı başlık altında ele almak mümkündür:

- İçsel kayıp verisi,
- Dışsal kayıp verisi,
- Senaryo analizi verileri,
- Önemli risk göstergelerine ait veriler,
- İç kontrollere dair veriler,
- Risk azaltımı araçlarına ait veriler.

1- İçsel Kayıp Verisi: Bankanın iş kollarında ve faaliyet birimlerinde meydana gelen operasyonel risk kayıp olayları, bu olayların nedenleri ve sonuçları hakkında bilgi edinmek amacıyla toplanan kayıp verisidir.

2- Dışsal Kayıp Verisi: Bankanın içsel kayıp verilerini desteklemek amacıyla kullanılan, diğer bankalar veya finansal kuruluşlar tarafından tecrübe edilen operasyonel risk kayıp olayları, olayların nedenleri ve sonuçları hakkında bilgiler içeren kayıp verisidir.

3- Senaryo Analizi Verileri: Bankaların karşı karşıya bulunduğu operasyonel risklerle ilgili olarak risk yönetimi uzmanlarının ve iş kollarındaki yöneticilerin uzman görüşleri alınarak operasyonel risk kayıp olaylarının meydana gelme olasılığı ve sıklığı konusunda gerçekleştirilen mantıklı değerlendirmeler sonucu elde edilen verilerdir.

4- Önemli Risk Göstergelerine Ait Veriler: Bu veriler, bankanın doğrudan kayıp verisine ulaşamadığı veya sayısallaştırılması zor operasyonel risklerin düzeyi ve ortaya çıkma potansiyeli hakkında dolaylı bilgiler verdiği düşünülen finansal veya finansal olmayan göstergelere ait verilerdir.

5- İç Kontrollere Dair Veriler: İç kontrollere dair veriler, bankanın iş ortamının koşulları ve bunlardan kaynaklanan operasyonel risklerle birlikte iç kontrollerin düzeyi, kalitesi ve etkililiğiyle ilgili göstergelere ait verilerdir.

6- Risk Azaltımı Araçlarına Ait Veriler: Sigortalamanın operasyonel risklerin yönetilmesinde bir risk azaltımı aracı olarak kullanılması halinde sigortanın kapsamı, koşulları ve yapılacak ödemeler başta olmak üzere sigortalama işlemlerine ait verilerdir.

D. Veri Kaynakları

Operasyonel risklerle ilgili veriler, verinin elde edildiği kaynak itibariyle banka içinden ve banka dışından elde edilen veriler olmak üzere iki ana grupta ele alınabilmektedir.

İçsel veriler, banka içerisindeki birimlerden toplanan operasyonel risklere ait verileri ifade etmektedir. Bankalar içsel kayıp verileri ile birlikte senaryo analizi verilerini, risk göstergelerine ve iç kontrollere ait verilerle sigortalama uygulamalarına ait verileri banka içinden sağlayabilmektedir. Bankanın faaliyetleri sırasında ortaya çıkan risk olaylarına ait veriler, operasyonel risk profilinin ortaya konulabilmesi için en gerekli ve kullanışlı verilerdir.

Operasyonel risk verileri, bankanın risk tanımlamalarına ve belirlenen risk kapsamına da bağlı olarak birçok farklı birim arasındaki etkileşim ile elde edilebilmektedir. Operasyonel risk kayıp olaylarına ait veriler bankaların organizasyon yapısına da bağlı olarak başlıca şu alanlardan elde edilebilecektir:

- Muhasebe ve mali kontrol
- İç kontrol
- Teftiş
- Risk yönetimi
- Bilgi sistemleri ve teknolojileri
- İnsan kaynakları
- Hukuk işleri
- Güvenlik (sistem, bilgi ve fiziki güvenlik)
- İdari hizmetler
- Esas faaliyet alanları ve operasyonel birimler

Ancak, sık gerçekleşen düşük maliyetli operasyonel kayıp olaylarının genellikle daha az dikkate alınması ve çok az sıklıkla gerçekleşen yüksek maliyetli kayıp olaylarına ait verilerin ise yetersiz sayıda olması, bankaya ait verilerin yalnız başına istatistiksel olarak güvenilir risk ölçümü için yeterli olmasını engellemektedir.

Dışsal kayıp verileri ise banka dışından sağlanan en belirgin operasyonel risk veri çeşidini oluşturmaktadır. Bu temel ikili ayrımın yanında banka dışından sağlanan veriler de veri kaynağına göre kendi içerisinde iki ana grupta ele alınabilmektedir: özel veriler ve kamuya açık bilgiler.

a. Dışsal Özel Veriler: Genellikle aynı sektörde faaliyet gösteren benzer diğer kuruluşların tecrübe ettiği, belli istatistiksel teknikler kullanılarak ve belli aşamalardan geçirilerek standartlaştırılan ve ortak bir veri tabanında toplanarak belirli gizlilik kuralları çerçevesinde kullanıma hazır hale getirilen operasyonel kayıp olaylarına ait verileri ifade etmektedir. Başka bankaların tecrübe ettiği kayıp olaylarına ait veriler, bankanın operasyonel risk profilinin belirlenmesinde ve risklerinin ölçümünde kendi verilerinden daha az uygun veriler olmasına rağmen, oldukça fazla sayıda olmaları sebebiyle ölçümlerde birçok ileri istatistiksel tekniğin kullanılabilmesine imkân sağlamaktadır. Diğer taraftan, dışsal veriler genellikle düşük sıklıkla gerçekleşen yüksek maliyetli kayıp olaylarına ait veriler olduğundan ve ilgili sektör veya grubun ortalama risk profilini yansıttığından, bu verilerin doğrudan bankanın risk profilinin belirlenmesinde kullanılması bazı sakıncaları da beraberinde getirmektedir.

b. Dışsal Kamuya Açık Veriler: Genellikle basın, yayın vb. yollarla kamuya açıklanan düşük sıklıkla gerçekleşen yüksek maliyetli kayıp olaylarına ait verileri ifade etmektedir. Bu tür veriler, genellikle sübjektif ve yönlendirilmiş veriler olduğundan, bunların doğrudan modelleme amacıyla kullanılması mümkün değildir.

II. VERİ VE VERİ TABANI MODELLEMESİNE İLİŞKİN TEMEL BİLGİLER

Operasyonel risklerin ölçülebilmesi için risk verilerinin toplandığı ve saklandığı bir veri tabanının bulunması gereklidir. Operasyonel riskin bankanın tamamına yönelik olduğu ve tüm faaliyet, süreç ve sistemlerle kişilere ait verilerin toplandığı dikkate alındığında, oluşturulacak veri tabanının kapsam ve içeriği ile temel mimarisinin nasıl olması gerektiği konusunda bir fikir elde edilebilecektir.

Veri tabanının oluşturulmasına yönelik bilgilerden önce konuyla ilgili temel kavramlar hakkında fikir edinilmesini sağlayacak bir takım temel bilgilerin verilmesi gerekmektedir. Bu bölümde, veri tabanı modellemesi, veri modellemesi, veri tabanı tasarımı gibi temel kavramlarla birlikte veri tabanı sisteminin işleyiş yapısı ve oluşturulma süreci konuları ele alınmaktadır[5].

A. Veri Tabanı Modellemesi

Veri tabanı, düzenli bir yapıya sahip bilgi kümesini ifade etmektedir. Bununla birlikte, günümüzde sadece bilgi işlem ortamındaki verileri ifade etmek amacıyla kullanılmaktadır.

Genelleştirilmiş veri tabanlarının yönetimi için hazırlanmış yazılımlar *"Veri Tabanı Yönetimi Sistemi (VTYS)"* olarak adlandırılmaktadır. Bu amaçla kullanılabilecek birçok farklı yazılım mimarisi bulunmaktadır. Örneğin, küçük tek kullanıcılı veri tabanları için tüm fonksiyonlar yalnızca bir yazılım tarafından yönetilebilirken, büyük ve çok kullanıcılı veri tabanları birçok yazılımın birlikte çalışmasını gerektirmekte ve yazılım mimarisi olarak da genellikle kullanıcı-servis sağlayıcı (client-server) mimarisi uygulanmaktadır.

VTYS'de, sistemin ön ucunda yer alan kullanıcılar (clients) veri girişi, sorgulama ve raporlama ile arka ucunda yer alan servis sağlayıcılar ise verilerin saklanması ve ön uçta yer alan kullanıcıların isteklerinin yerine getirilmesi ile ilgilenirler. Tarama ve sıralama ise genellikle hizmet sağlayıcı tarafından yerine getirilmektedir. Halen tek bir dosyada saklanan basit tablolardan oluşan küçük veri tabanlarından milyonlarca kayıttan oluşan ve bunların disk sürücülerinde veya elektronik saklama cihazlarında saklandığı çok büyük veri tabanlarına kadar birçok farklı veri tabanı uygulaması mevcuttur.

Modern veri tabanlarına benzeyen ilk veri tabanı 1960 yılında bu alanın öncüsü konumundaki Charles Bachman tarafından geliştirilmiştir. İlk veri tabanından sonra ortaya

[5] Veri tabanı ve veri modellemesi ile veri tabanı tasarımına ilişkin olarak bu bölümde verilen temel bilgiler Batini vd (1991), Date (1990), Fleming vd. (1989), Kroanke (1983), Reingruber, Gregory (1994), Simsion (1994) ve Teory (1999)'den derlenmiştir. Daha detaylı bilgi için bu kaynaklardan yararlanılabilir.

çıkan iki temel veri tabanı modeli *"ağ (network) modeli"* ve bunu takip eden *"hiyerarşik model"*dir. Daha sonra bu modellerin saltanatına, 1976 yılında ilk defa Peter Chen tarafından geliştirilen ve halen her alanda kullanılan *"ilişkisel (relational) veri tabanı modeli"* son vermiştir. Günümüzde, ilişkisel modelin yanında yeni geliştirilmekte olan *"nesneye yönelik (object-oriented) veri tabanı modeli"* de kullanılmaktadır.

Veri yapılarının modellenmesinde birçok farklı teknik kullanılmaktadır. Bazı modeller belli bazı veri tabanı yönetimi sistemlerinde diğerlerine kıyasla daha kolay uygulanabilmektedir. Bir mantıksal model için birden fazla fiziki uygulama mümkün bulunmaktadır. Bunun bir örneği de ilişkisel modeldir.

İlişkisel model, bir veri tabanının yönetilmesinde kullanılan, önermeye dayalı mantığa ve küme teorisine dayanan bir veri modelidir. Bu modelin temel varsayımı, tüm verilerin matematiksel ilişkilerle temsil edildiğidir. Matematiksel modelde bilinmeyen (null) değerler bulunmamakta, verilerle ilgili uslamlama iki değer alan önermeli mantıkla yapılmaktadır. Diğer bir ifade ile her bir önerme için "doğru" ve "yanlış" olmak üzere iki olası değerlendirme yapılmaktadır. Veriler, ilişkisel matematik (relational calculus) ve cebir ile işlem görmektedir.

İlişkisel modelin temel prensibi, tüm bilgilerin ilişki içindeki veri değerleri ile temsil edildiğine ilişkin *"bilgi prensibi*"dir. Dolayısıyla, ilişki değişkenleri tasarım anında birbirleri ile ilişkili değildir. Tasarımı gerçekleştiren modelci birçok ilişkili değişken için aynı tanım kümesini kullanabilmekte, bir ilişki atfı diğerine bağlı ise bu bağımlılık referans bütünlüğü ile sağlanmaktadır.

Diğer veri tabanı modelleri, hiyerarşik model ve ağ modelidir. Halen, özellikle sistem mimarisinin değiştirilmesi ve ilişki modeline geçilmesinin sistemin karmaşıklığı nedeniyle maliyetli olduğu bazı sistemler bu eski veri tabanı mimarilerini kullanmaktadır. Bu eski modellerin yanında yeni gelişmekte olan nesneye yönelik veri modelleri, uygun veri tabanı yönetim sistemi olmaktan ziyade bu sistemlerin inşasında kullanılan araç konumundadır.

İlişki modeli formel anlamda ilk veri tabanı modelidir. İlişki modelinin tanımlanmasının ardından hiyerarşik ve ağ veri tabanlarını ifade etmek amacıyla formel olmayan modeller *(hiyerarşi* ve *ağ veri modelleri*) geliştirilmiştir. Hiyerarşik ve ağ veri tabanları ilişkisel veri tabanlarından önce mevcut iken, bunların karşılaştırılabilmesine bir temel oluşturabilmek amacıyla "*model"* olarak ifade edilmesi, ilişki modelinden sonra gerçekleşmiştir.

B. Veri Modellemesi

Veri modeli, bir bilgi sisteminde veya veri tabanı yönetimi sisteminde verinin kavramsal olarak ne şekilde temsil edileceğini gösteren modeli ifade etmektedir. Diğer bir ifade ile veri modeli, veri yapılarının bir veri tabanının gerektirdiği şekilde kavramsal gösterimini ifade etmektedir. Buradaki veri yapıları veri nesnelerinden, veri nesneleri arasındaki ilişkilendirmelerden ve nesneler üzerindeki işlemlerin gerçekleştirilmesini sağlayan kurallardan oluşmaktadır. Veri modeli, veri üzerinde hangi işlemlerin gerçekleştirildiğine değil hangi verinin gerektiğine ve bunların ne şekilde tasnif edildiğine odaklanmaktadır. Veri modeli bir anlamda binanın ne şekilde inşa edileceğini değil, mimarın hazırladığı mimari planları göstermektedir.

Veri modeli için herhangi bir yazılım ve donanım sınırlaması bulunmamaktadır. Veri modeli, bir veri tabanının veriyi ne şekilde göreceğini göstermekten ziyade kullanıcıların gerçek dünyada veriyi gördükleri şekliyle verinin temsil edilmesine odaklanmaktadır. Veri modeli, bir anlamda, gerçek dünyadaki olayları ve süreçleri oluşturan kavramlarla bu kavramların veri tabanı içerisinde fiziki temsilleri arasında köprü vazifesini görmektedir.

Veri modelinin oluşturulmasında iki temel yöntem kullanılmaktadır: Varlık-İlişki (Entity-Relationship, ER) yaklaşımı ve nesne (object) modelidir.

ER modeli, kavramsal veri modellerinin genel hatlarıyla tasvir edilmesinde kullanılan bir veri modelidir. ER modeli, bu tür veri modellerinin gösteriminde ER diyagramları şeklinde grafik gösterim sağlamaktadır. Bu tür veri modelleri genellikle bilgi sistemi tasarımının ilk aşamasında kullanılmaktadır. Bu modeller, örneğin, gereksinim analizleri esnasında bilgi gereksinimleri ile veri tabanında saklanacak bilgi türünün tasvir edilmesinde kullanılmaktadır.

ER modelinde, tanımlanan nesneler arasındaki ilişkiler ve yapılan işlemler ön planda iken nesneye dayalı modellerde, işlemlerden ziyade nesneler ön planda tutularak modelleme işlemi gerçekleştirilmektedir.

C. Veri Tabanı Tasarımı

Veri tabanı tasarımı, bir organizasyonda tanımlanmış bir uygulama grubu için kullanıcıların bilgi ihtiyaçlarının karşılanabilmesi amacıyla bir veya birden fazla veri tabanının mantıksal ve fiziksel yapısının tasarımının gerçekleştirilmesini ifade etmektedir. Veri tabanı tasarımı süreci beş aşamada ele alınabilmektedir (Opel, 2004):

1. Planlama ve analiz

2. Kavramsal tasarım
3. Mantıksal tasarım
4. Fiziksel tasarım
5. Uygulama

İlk aşama olan planlama ve analiz aşamasında, veri ihtiyaçları ve veri tabanı amaçları göz önünde bulundurularak tasarım sürecine ait faaliyetler planlanır. Planlamanın yanında veri ihtiyaçları belirlenir.

İkinci aşama olan kavramsal tasarım sürecinde, veri modellemesi gerçekleştirilir.

Üçüncü aşamayı oluşturan mantıksal tasarımda, verilerin ne şekilde işleneceği ve hangi işlemlerin gerçekleştirileceğine dair fonksiyonlarla birlikte veri tabanı işlemlerinin tasarımı gerçekleştirilir.

Dördüncü aşama olan fiziksel tasarım aşamasında, kavramsal tasarımı gerçekleştirilen veri modeli ile mantıksal tasarımı gerçekleştirilen fonksiyon modelinin veri tabanı uygulamalarına yönelik fiziksel yapısı oluşturulur.

Fiziki olarak oluşturulan veri tabanının son aşama olan uygulama aşamasında belirlenen amaçlar doğrultusunda kullanımı gerçekleştirilir.

D. Veri Tabanı Sisteminin Temel Yapısı

Operasyonel risk verilerinden oluşan ve operasyonel risk ölçümü ve yönetimi amaçlarına hizmet etmek üzere oluşturulan operasyonel risk veri tabanı, ***"Veri Tabanı Yönetimi Sistemi" (VTYS)*** veya daha kısa ifade ile ***"Veri Tabanı Sistemi"*** olarak da adlandırılan bir sistem tarafından yönetilecektir. Bu sistem bankanın tüm iş kolları ve faaliyetlerinden topladığı risk verilerinin işlenmesi ve etkin olarak yönetilmesi amacıyla geliştirilen güçlü yazılımlar tarafından idare edilmektedir. Kullanılan yazılımlar, en karmaşık yazılım programları arasında yer almaktadır.

Ullman-Widom (2001)'a göre bir veri tabanı sistemi başlıca şu imkânları sağlamalıdır :

(a) ***Veri Tabanının Geliştirilebilmesi***: Sistem, kullanıcıların veri tanımlama dili (data definition language, DDL) olarak adlandırılan özel bir programlama dili kullanarak mevcut veri tabanını daha da geliştirmesine veya yeni veritabanları geliştirmesine ve

veri modelinin temel şemasını (verinin mantıksal yapısını) değiştirmesine imkân sağlamalıdır.

(b) ***Verilerin Saklanmasını Destekleme***: Sistem, risk verilerini kullanarak analiz ve ölçüm gerçekleştiren süreçlerden bağımsız olarak bir dosyalama sistemine benzer şekilde büyük miktardaki risk verisinin saklanmasını sağlamalıdır. Sistem, veri saklama konusunda dosyalama sisteminin ötesine geçerek kullanıcıların birçok veriye sistematik bir şekilde ulaşmasını ve bunlar üzerinde işlem gerçekleştirmesini sağlamalıdır.

(c) ***Programlama Arayüzü***: Sistem, kullanıcının güçlü bir sorgu dili (query language, QL) veya veri işleme dili (data-manipulation language, DML) kullanan bir uygulama programı ile sisteme girmesine, yeni veri eklemesine, veri çıkarmasına ve mevcut verileri değiştirmesine imkân sağlamalıdır.

(d) ***İşlem Yönetimi***: Sistem, risk verilerine aynı anda farklı süreçlerin veya kullanıcıların girişine ("işlem" olarak adlandırılmaktadır) ve birbirini etkilemeksizin verileri kullanmasına imkân sağlamalıdır. Sistemin temel özellikleri olan "izolasyon" (işlemlerin birbirinden ayrı ve birbirini bozucu etkide bulunmaksızın gerçekleşmesi) ve "atomicity" (işlemlerin ya hepsinin birlikte gerçekleşmesi ya da hiçbirisinin gerçekleşmemesi koşulu) sayesinde aynı anda sisteme girişlerden kaynaklanan sorunlar ortadan kaldırılabilmelidir.

Genel olarak bir veri tabanı yönetimi sisteminin sahip olması gereken temel unsurlar ile sistemin temel işleyişine yönelik şemaya Ek 5'de yer verilmektedir.

Operasyonel risk veri tabanının mimarisi her bir bankanın ihtiyaçlarına, kullandığı mevcut bilgi işlem sistemine, sistemlerin üzerine inşa edildiği bilgi işlem sistemi mimarisine, veri tabanının ilişkilendirildiği risk ölçümü ve yönetimi sistemlerinin özelliklerine bağlı olarak farklılıklar gösterebilecektir. Ancak, operasyonel risk veri tabanının bu faktörlerden kaynaklanan farklılıkları da göz önünde bulundurularak genel anlamda şu temel unsurlara sahip olması gerekmektedir:

- Veri tabanı yöneticisi
- Kullanıcılar/Uygulama Programları
- Veri tanımlama ve veri değiştirme dili komutları (DML ve DDL)
- Sorgu işlemcisi
- Saklama yönetimi
- İşlem yönetimi

E. Veri Tabanının Oluşturulması Süreci

Operasyonel risk veri tabanı sistemleri konusundaki çalışmaları, veri tabanının tasarımı ve programlanması ile veri tabanı sisteminin uygulamaya konulması olmak üzere üç ana bölümde ele almak mümkündür (Ullman-Widom, 2001):

a. Veri Tabanının Tasarımı

Veri tabanının tasarımı, veri tabanının kavramsal olarak tasarlanmasını ifade etmektedir. Kavramsal tasarım, veri modellemesinden meydana gelmektedir. Tasarım sürecinde ele alınması gereken başlıca konular şunlardan oluşmaktadır:

- Amaca uygun bir veri tabanının ne şekilde geliştirilebileceği
- Veri tabanına ne türlü verilerin dahil edileceği
- Bilgilerin ne şekilde yapılandırılacağı
- Veri türleri ve veri değerleri konusunda yapılan varsayımlar
- Verilerin birbirleriyle ilişkilendirilmesi

b. Veri Tabanının Programlanması

Veri tabanının programlanması, hangi tür verilerin ne şekilde ele alınacağı ve birbirleriyle nasıl ilişkilendirileceğine yönelik olarak tasarımı gerçekleştirilen veri modeli üzerinde programlamaların gerçekleştirilmesidir. Programlama sürecinde ele alınması gereken başlıca konular şunlardan oluşmaktadır:

- Veri tabanında sorguların ve diğer operatörlerin nasıl ifade edileceği
- VTYS'nin işlemler, kısıtlar gibi yeteneklerinin ne şekilde kullanılacağı
- Veri tabanı programlamasının geleneksel programlama ile ne şekilde bir araya getirileceği.

c. Veri Tabanı Sisteminin Uygulanması

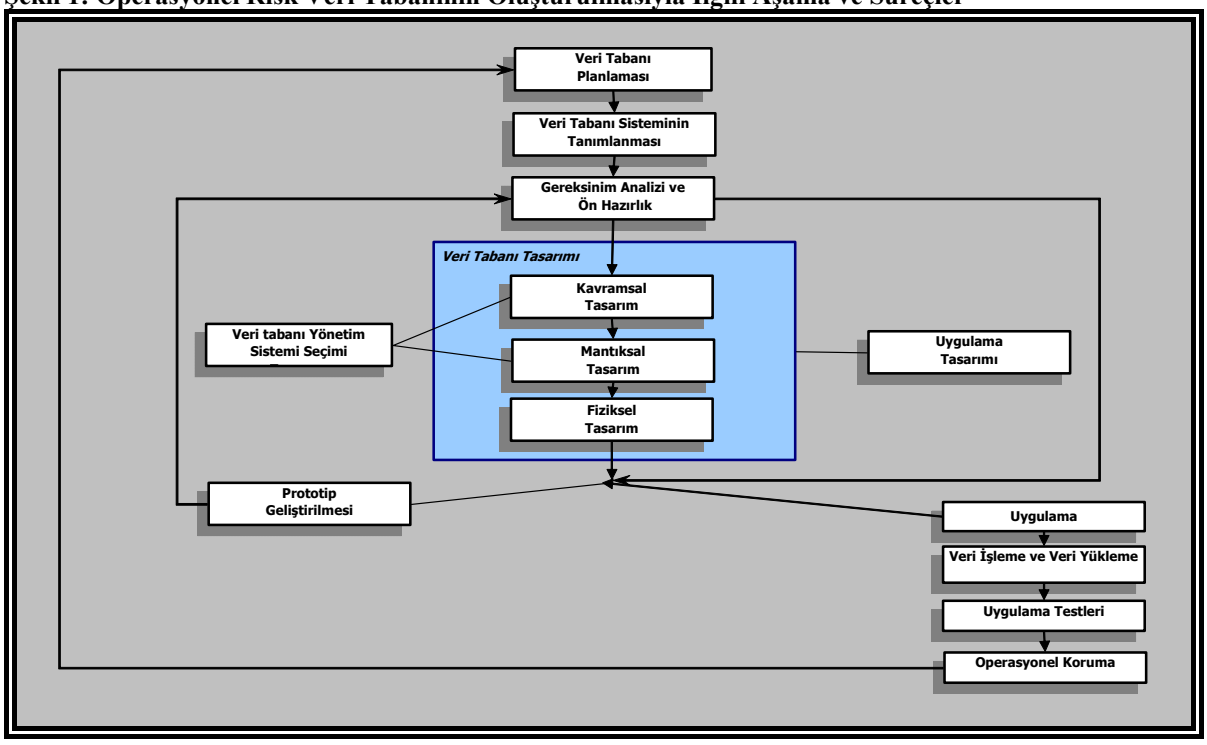
Veri tabanı sisteminin uygulanması, kavramsal ve mantıksal tasarımı gerçekleştirilen veri tabanı sisteminin uygulanması ile ilgili olarak fiziki tasarımın yapılması ve fiziki yapının oluşturulma sürecini ifade etmektedir.

III. OPERASYONEL RİSK VERİ TABANI SİSTEMİNİN KURULMASI

Operasyonel risk veri tabanının oluşturulması, yoğun bir şekilde kaynak ve teknoloji kullanımı gerektirmektedir. Operasyonel risklerin sayısallaştırılması ile operasyonel risk verilerinin tanımlanması ve toplanmasında karşılaşılan zorluklar ve sorunlar, veri tabanının tasarlanmasını ve uygulanmasını daha da önemli hale getirmektedir.

Operasyonel risk veri tabanının oluşturulması, Şekil 1'de yer verilen iş akışlarına uygun olarak gerçekleştirilebilir. İlk olarak veri tabanına yönelik planlama faaliyetleri ile başlayan süreçte oluşturulmak istenilen veri tabanı sistemi belirlenmeli ve ana unsurları tanımlanmalıdır.

Şekil 1: Operasyonel Risk Veri Tabanının Oluşturulmasıyla İlgili Aşama ve Süreçler



Tasarım sürecine başlamadan evvel gereksinim analizi ve operasyonel risk verileriyle ilgili ön hazırlık faaliyetleri gerçekleştirilmelidir. Gereksinim analizi tasarım süreci boyunca ve süreç sonunda tekrar gözden geçirilerek gerekli düzeltme veya değişiklikler yapılabilir.

Veri tabanı, tasarımın üç boyutu itibariyle kavramsal, mantıksal ve fiziksel olarak tasarlanmalıdır. Veri tabanı modeline bağlı olarak kavramsal ve mantıksal tasarım değişeceğinden benimsenen veri tabanı modelinin seçimi önemli bir aşamadır. Veri tabanının uygulamaya yönelik tasarımı da bu aşamada yapılmalıdır.

Operasyonel risk veri tabanının tasarlanması süreci; tüm sürecin planlanması ve veri tabanı için gerekli veri ve diğer kaynakların belirlenmesi ile başlamakta, operasyonel risk veri modelinin tasarlanmasından oluşan kavramsal tasarım süreci ile devam etmektedir. Kavramsal tasarım sürecini, risk verilerinin işlenmesine yönelik fonksiyonların ve yöntemlerin tasarlandığı mantıksal tasarım süreci ve veri tabanının fiziksel yapısının oluşturulduğu fiziksel tasarım süreci takip etmektedir. Son aşamada ise, kavramsal, mantıksal ve fiziksel tasarımı gerçekleştirilmiş veri tabanı, belirlenen amaçlar doğrultusunda uygulamaya konulmaktadır.

Prototip kullanımı politikası benimsenmişse, istenen düzeye ulaşılıncaya kadar tasarımın geliştirilmesi süreci devam ettirilebilir.

Tasarımı tamamlanan veri tabanı sistemine veriler yüklenmeli, yüklenen veriler işlenmeli ve sistem amaca uygun niteliklere sahip veriler elde etmeye dönük olarak uygulama testlerine tabi tutulmalıdır.

Tasarımı tamamlanan ve tüm işleyiş testlerinden geçen veri tabanı sisteminin devamlılığını sağlamaya yönelik olarak sürekli bakım, koruma ve geliştirme faaliyetleri gerçekleştirilmelidir.

Bu bölümde, operasyonel risk veri tabanının tasarlanması süreci aşamalar ve her bir aşamada gerçekleştirilmesi gereken faaliyetler itibariyle ele alınacaktır.

1. Aşama- Planlama

Planlama aşamasında, bankanın operasyonel risk ölçümü ve yönetimi sisteminin gerektirdiği kapsam, içerik ve yeterlilikte veri ve veri tabanı yapısının oluşturulabilmesi için gerekli faaliyetler ile tahsis edilmesi gerekli kaynaklarla ilgili planlama işlemi gerçekleştirilir.

Planlamada veri tabanının amaçları belirlenerek, bu amaçların niçin önemli olduğu ve bu amaçların elde edilme yolları ortaya konulur.

Veri tabanı tasarımına yönelik planların geliştirilmesinde, oluşturulması hedeflenen veri tabanının büyüklüğü, işlevselliği, kapsamı, içeriği ve analiz kabiliyetlerine yönelik yönetim politikalarıyla, hedeflenen veri tabanı için gerekli kaynak-maliyet unsurları esas alınır.

Hedeflenen veri tabanının genel çerçevesinin belirlenmesinin ardından tasarım süreçleri, süreçlerde yapılması gereken faaliyetler ve kaynak tahsisi konularında planlar hazırlanır. Veri

tabanının oluşturulması tüm unsurları ile bir proje olarak tanımlanarak projeye ait yol haritası oluşturulur. Hazırlanan yol haritası, aşamalara ait planların mümkün olduğunca detaylandırılması suretiyle kaynak tahsisinin etkin bir şekilde yapılmasında esas alınır.

2. Aşama- Veri Tabanının Tasarımı: Kavramsal Tasarım

Operasyonel risk veri tabanının kavramsal tasarımı süreci veri modellemesinden oluşmaktadır. Veri modeli, veri tabanında hangi verilerin saklanması gerektiği, fonksiyon modeli ise verilerin nasıl işleneceği, hangi işlemlerden geçirileceği üzerine odaklanmaktadır.

Kavramsal tasarım süreci ilişkisel veri tabanı modeli kapsamında ele alındığında, veri modeli ilişkisel tabloların, fonksiyon modeli ise bu tablolara girerek tablolar üzerinde işlemler gerçekleştirecek sorguların tasarlanmasında kullanılmaktadır. Fonksiyon modeline veri tabanının programlanmasına yönelik araçları ve faaliyetleri içerdiğinden ilgili kısımda yer verilecektir.

Veri modellemesi***, "aşağıdan yukarıya"*** bir modelleme sürecidir. İlk olarak, varlıkları ve ilişkileri temsil eden bir temel model geliştirilir. Bunun ardından, modele nitelikler ve risk yönetimi kuralları da ilave edilerek modelin daha detaylı hale gelmesi sağlanır.

Operasyonel risk veri modeli, veri tabanında risk verilerinin kavramsal olarak ne şekilde ifade edileceğini gösteren modeldir. Veri modeli, veri üzerinde hangi işlemlerin gerçekleştirildiğine değil hangi verinin gerektiğine ve bunların ne şekilde tasnif edildiğine odaklanmaktadır.

Veri ve veri tabanı modelinin oluşturulmasında halen her alanda kullanılan ER modeli esas alınmalıdır. ER modeli gerektiğinde nesne modeliyle de desteklenmelidir.

A. Veri Modellemesi ve Veri Modelinin Unsurları

Veri modellemesi, veri tabanının geliştirilmesi sürecinin en fazla emek gerektiren ve zaman alan aşamasını oluşturmaktadır. Veri tabanının başarısı, veri modelinin başarısı ile çok yakından ilişkilidir. Veri modeli olmadan geliştirilecek bir veri tabanı, mimari ve yapı planı olmadan inşa edilmeye çalışılan bir binaya benzeyecektir.

Operasyonel risk veri modelinin amacı, veri tabanının gerektirdiği risk verilerinin tüm unsurlarının veri nesneleri olarak veri tabanında tam ve doğru bir şekilde temsil edilmesini sağlamaktır.

Veri modelinin yeterli düzeyde detaylandırılması, veri tabanını geliştirenlerin fiziksel veri tabanını oluşturmaları esnasında veri modelini mimari bir plan olarak kullanılabilmelerini sağlamaktadır. Veri modelinde yer verilen bilgiler ilişkisel tabloların, temel anahtar (pk) ve yabancı anahtarların (fk), saklanmış prosedürlerin ve harekete geçirici tetiklerin tanımlanmasında kullanılacaktır. Yetersiz bir şekilde geliştirilmiş bir veri tabanı uzun vadede üzerinde daha çok zaman harcanmasını gerektirecektir. Dikkatli bir planlama ve analiz yapılmadan oluşturulan bir veri tabanı kritik önemdeki raporların üretilmesini ve sağlıklı risk ölçümü yapılmasını sağlayacak verileri göz ardı edebilecek, yanlış veya tutarsız sonuçların ortaya çıkmasına neden olabilecek ve kullanıcının isteklerine yanıt veremeyecektir.

Veri modellemesi aşamasının girdileri, planlama ile gereksinim analizi aşamalarından elde edilmektedir. Modelci, operasyonel risk yöneticileri ve uzmanları ile birlikte mevcut dokümanların incelenmesi ve son kullanıcılarla yapılan görüşmelerin ardından veri tabanının gereksinimlerine dair bilgilerin toplanması işlerini yapar.

Veri modellemesi aşamasının başlıca iki çıktısı bulunmaktadır. Bunlardan ilki, veri yapılarını resmeden ER diyagramıdır. Diyagram, öğrenilmesi ve anlaşılması daha kolay olduğundan son kullanıcılara modelin tanıtımını oldukça kolaylaştırır. İkincisi ise bir veri dokümanıdır. Bu doküman veri tabanının gerektirdiği veri nesnelerini, ilişkileri ve kuralları ayrıntılı bir şekilde ele almaktadır. Veri dokümanında yer alan detaylı bilgiler veri tabanının programlanmasında ve fiziksel tasarımında kullanılır.

B. Gereksinim Analizi

Veri tabanının oluşturulmasının en önemli aşamalarından birisi gereksinimlere dair analizin gerçekleştirilmesidir. Veri ve veri tabanı modelinin kapsamını, içeriğini, yeteneklerini ve bankanın risk ölçümü ve yönetimi amaçlarına uygun olarak gerçekleştirilmesini büyük oranda bu analizin başarısı belirlemektedir.

Gereksinimlerin belirlenmesi, *operasyonel kavram dokümantasyonu*, *sistem mühendisliği* gibi isimlerle de anılan bu analizle veri tabanı projesi ihtiyaç, amaç, hedef ve kısıtlar göz önünde bulundurularak şekillendirilir ve böylece projenin temel çerçevesi belirlenir.

Veri tabanı projesini yürüten modelcilerin veri tabanından nihai kullanıcı olarak yararlanacak olan operasyonel risk ölçümü ve yönetimi uzmanlarıyla, risk yöneticileriyle ve diğer ilgili taraflarla birlikte çalışmak suretiyle veri tabanında bulunması gerekli verileri ve bu verilerin kaynaklarını belirlemeleri gerekmektedir.

Gereksinim analizinin gerçekleştirilebilmesi için öncelikle şu konularda yeterli miktarda bilginin sağlanması gereklidir.

- Banka yönetiminin operasyonel risk veri tabanı konusundaki politika ve stratejileri
- Yönetimin veri tabanı projesinin gerçekleştirilmesi konusundaki kararlılığı, bu amaçla banka çapında yürütülecek çalışmalara desteği
- Veri tabanının bankanın risk yönetim sistemi içerisindeki yerinin ne olmasının amaçlandığı ve beklendiği
- Veri tabanının kapsamı, içeriği, detay düzeyi, kullanılacak teknolojiler, ne tür veriler üreteceği konularındaki beklentiler
- Risk yönetimi sistemi ile ne şekilde ilişkilendirileceği, hangi analizlerin gerçekleştirilebilmesi için veri üretmesinin beklendiği
- Bankanın kullandığı (kullanacağı) risk ölçüm sisteminin temel özellikleri, kullanılan modellere girdi olarak ne tür verilerin, hangi kapsamda ve nitelikte sağlanması gerektiği
- Kredi riski, piyasa riski ve diğer risklerin veri tabanları ile ne şekilde ilişkilendirilmesinin beklendiği
- Bankanın mevcut bilgi işlem sisteminin temel özellikleri, mevcut sistemlerle oluşturulması planlanan veri tabanının birbirlerine uyum düzeyi, olası uyumsuzluklar, uyumsuzlukların ne şekilde ortadan kaldırılmasının planlandığı
- Kullanıcıların veri tabanından beklentileri

Bankanın ihtiyaç ve beklentilerine en uygun veri tabanının tasarlanabilmesi için gerekli bu bilgiler, kullanıcılarla yapılacak görüşmelerden; yönetimle ve operasyonel risk uzmanlarıyla yapılacak toplantılardan; yönetimin politika, strateji ve uygulama kararlarıyla ilgili yazılı belgeler ile bankanın sistem ve süreçlerine ait uygulama usulleri, yazılı dokümanlar ve teknik belgelerin incelenmesinden elde edilmelidir.

Operasyonel risk veri tabanı için gerçekleştirilecek gereksinim analizinin (GA) temel amaçları şunlardır:

- Ana hatlarıyla belirlenen ilk veri nesneleri itibariyle veri tabanının veri gereksinimlerinin belirlenmesi
- Bu nesnelerle ilgili bilgilerin belirlenmesi ve sınıflandırılması
- Nesneler arasındaki ilişkilerin tanımlanması ve sınıflandırılması

- Veri tabanında gerçekleştirilecek işlemlerin türlerinin ve verilerle işlemler arasındaki etkileşimlerin belirlenmesi
- Risk verisinin bütünlüğünü ve doğruluğunu kontrol altında bulunduran kuralların tanımlanması

Gereksinim analizi, veri modellemesinin gerçekleştirilmesi ile eş zamanlı olarak gerçekleştirilir. Verilerin toplanması ile eş zamanlı olarak veri nesneleri varlık, nitelik (attributes) veya ilişki olarak tanımlanır ve sınıflandırılır, isimlendirilir ve son kullanıcının aşina olduğu terimlerle ifade edilir. Bu işlemi takiben veri nesneleri ER diyagramı kullanılarak modellenir ve analiz edilir. Hazırlanan diyagram modelci ve son kullanıcılar tarafından tamlık ve doğruluk düzeyinin belirlenmesi amacıyla gözden geçirilebilir. Model doğru değilse, gerektiğinde ilave bilgi sağlanmasının ardından düzeltilir. Modelin gözden geçirilme ve düzeltilme döngüsü modelin doğruluğunun sağlanmasına kadar devam ettirilir.

Operasyonel risk veri modelinin oluşturulabilmesi için öncelikle risk tanımının belirlenmesi, risk verilerinin sınıflandırılması ve veri kaynaklarının belirlenmesi gereklidir. Bu aşamaları takiben verilerin toplanması süreci başlatılarak veri modelinin tasarımı aşamasına geçilir.

C. Ön Hazırlık

Veri tabanının tasarım aşamalarına geçmeden evvel bu aşamalarda kullanılacak bazı temel unsurlarla ilgili ön hazırlıkların yapılması gereklidir. Bu amaçla öncelikle maruz bulunulan operasyonel risklerin belirlenmesi ve bunlara ait tanımların yapılması gerekmektedir. Tanımlamayı takiben verilerin sınıflandırılması, veri kaynaklarının belirlenmesi ve bu bilgiler kullanılarak veri modelinin oluşturulması gerekmektedir.

1. Operasyonel Risk Tanımının Belirlenmesi

Operasyonel riskin tanımı, her kuruluşun riski ele alış biçimiyle birlikte, risk ölçüm ve yönetim stratejisine göre de farklılıklar gösterebilecektir.

Operasyonel risk yönetimi süreci riskin tanımlanması, sayısallaştırılarak ölçülmesi, riskin izlenmesi, riskin azaltılması ve kontrol edilmesi olarak sıralanabilecek başlıca dört temel süreçten meydana gelmektedir. Bankaların birbirlerinden farklı özellikleri de dikkate alınarak geliştirilecek operasyonel risk tanımları bankanın operasyonel risk yönetiminin başlangıç noktasını ve temelini oluşturacaktır.

Bu nedenle, operasyonel riskin tanımlanması aşamasında kuruluşun riski ele alış biçimine, risk alma eğilimine, risk taşıma kapasitesine, risk profiline, risk ölçümü ve yönetimi strateji ve politikasına göre kapsamlı bir risk tanımının benimsenmesi büyük önem taşımaktadır.

2. Verilerin Sınıflandırılması

Veri modelinde kullanılacak verilerin belirlenmesi ve bu verilerin sistematik bir şekilde sınıflandırılması veri tabanının kapsamlılığı ve amaçlara uygunluğunun sağlanmasında önem taşımaktadır. Bu amaçla, öncelikle risklerin ölçümünde ve yönetiminde operasyonel risklerle ilgili hangi verilerin kullanılabileceğinin dikkatli bir şekilde belirlenmesi gereklidir.

Operasyonel risklerle ilgili olarak başlıca beş ana grup altında veri toplanabilir[6]. Bunlar;

- Kayıp verileri (içsel ve dışsal)
- Nedensellik verileri
- Önemli risk göstergelerine ait veriler
- İç kontrollerle ilgili veriler
- Riski azaltma ve riskten korunma araçlarına ait veriler

Kayıp verileri, gerçekleşen operasyonel risk kayıp olayına ait verileri ifade etmektedir. Kayıp verileri üç boyutlu olarak ele alınmalıdır: Operasyonel kayıp olayı, kayıp olayının ortaya çıkmasına neden olan etkenler ve olay sonucu ortaya çıkan etki.

Operasyonel risk olaylarının ortaya çıkmasına neden olan etkenlere ait veriler riskin yönetilebilmesi için öncelikli olarak gerekli verilerdir. Nedensellik verileri kapsam ve nitelik açısından bankanın risk yönetimine yaklaşımına bağlı olarak farklılık gösterebilecektir. Operasyonel riskin nedenlerine yönelik olarak Basel Komitesinin belirlediği ana risk alanları esas alınarak ayrıntılı sınıflandırmalar geliştirilebilir[7].

Operasyonel riskin nedenleri konusunda genel kabul gören sınıflandırmaya göre dört ana risk alanı bulunmaktadır:

- Süreçler

[6] Basel Komitesinin operasyonel risk verilerine ve verilerin sınıflandırılmasına yaklaşımına yönelik değerlendirmeler için bakınız Mazıbaş (2005d).

[7] Operasyonel risklerin nedenlerine ilişkin olarak İngiliz Bankacılar Birliğinin (BBA) süreçler, sistemler, insanlar ve harici etkenlerden kaynaklanan operasyonel risk kayıplarına ilişkin sınıflandırması esas alınarak tasarlanan sınıflandırma Ek 3'de yer almaktadır. Bu sınıflandırma, bankaların dört temel operasyonel risk alanı itibariyle alt sınıflandırmalar geliştirmelerine yardımcı olmak amacıyla konulmuştur. Bankalar bu sınıflandırmalardan yola çıkarak kendi yapılarına en uygun nedensellik verisi sınıflandırmasını geliştirebilirler.

- Sistemler
- İnsanlar
- Dışsal etkenler

Operasyonel risk kayıp olayı ile ilgili olarak toplanacak veriler Basel Komitesinin belirlediği yedi ana risk olayı grubu altında sınıflandırılabilir[8]:

- Banka içi hile ve dolandırıcılık olayları
- Banka dışı hile ve dolandırıcılık olayları
- İstihdam uygulamaları ve işyeri güvenliğiyle ilgili kayıp olayları
- Müşteriler, ürünler ve iş uygulamalarına dair kayıp olayları
- Fiziki varlıklara verilen zararlarla ilgili olaylar
- Faaliyetlerin durması ve sistem hatalarına dair kayıp olayları
- İşleme, teslimat ve süreç yönetimine dair kayıp olayları

Operasyonel kayıp olayı nedeniyle ortaya çıkan etkiler konusundaki sınıflandırmada da Basel Komitesinin belirlediği altı kayıp grubu kullanılabilir:

- Varlık değerindeki azalmalar
- Rücu edilmesinden kaynaklanan kayıplar
- İade ve kaybı tazminler
- Yasal sorumluluk
- Denetim otoritesi ve mevzuata uyumsuzluk nedeniyle alınan cezalar
- Aktiflerden veya aktiflere verilen hasarlardan kaynaklanan kayıp

Operasyonel kayıp olayıyla ilgili olarak toplanacak veriler asgari olarak şu bilgileri içermelidir:

- Tanımlanan kayıp olayının türü
- Olayın gerçekleşmesine ilişkin kısa açıklama
- Olayın gerçekleştiği iş kolu, birim veya yer
- Olayın gerçekleşmesine neden olan etkenler
- Olay nedeniyle ortaya çıkan etkiler

[8] Daha detaylı olay sınıflandırması için Ek 1'deki sınıflandırmadan yararlanılabilir.

- Kaybın finansal boyutu
- Gerçekleşme tarihi
- Devam süresi
- İlk tespit edilme tarihi
- Olayın gerçekleşmesi ile tespit edilmesi arasında geçen süre
- Mevcut ise sigortaya bildirim işleminin yapıldığı tarih
- Takip eden yasal işlemler
- Kayıp azaltılmış ise kaybın ne kadarının karşılandığı

Önemli risk göstergelerine ait bilgiler, operasyonel risk olaylarının meydana gelme sıklığını veya olay sonucu ortaya çıkan kaybın boyutunu etkilediği ve operasyonel risk hakkında dolaylı bilgi verdiği değerlendirilen finansal veya finansal olmayan değişkenlere ait bilgileri ifade etmektedir.

İç kontrollere ait bilgiler ise, operasyonel risk olaylarının meydana gelme sıklığını veya olay sonucu ortaya çıkan kaybın boyutunu etkileyen bankanın iç denetim (iç kontrol ve teftiş) ve risk yönetim sistemlerinin kalitesine, etkinlik düzeyine ve riski azaltma yeteneğine ilişkin bilgiler veren kontrol göstergelerini ifade eder.

Sigortalama bilgileri ise, sigortalamanın operasyonel risklerin yönetilmesinde bir risk azaltımı aracı olarak kullanılması halinde sigortanın kapsamı, koşulları ve yapılacak ödemeler başta olmak üzere sigortalama işlemlerine ait verilerdir.

Operasyonel risk göstergelerine ve kontrol ortamına ilişkin sınıflar, bankanın benimsediği risk ölçümü ve yönetimi yaklaşımına bağlı olarak gerek kapsam gerekse de içerik açısından farklılıklar gösterebilecektir. Bu nedenle, bunlarla ilgili veri sınıflandırmalarının geliştirilmesinde benimsenen risk yönetimi yaklaşımı esas alınmalıdır.

3. Veri Kaynaklarının Belirlenmesi

Operasyonel risk veri kaynaklarının belirlenmesi, benimsenen risk tanımlarından ve belirlenen risk sınıflarından hareketle gerçekleştirilebilir. Operasyonel risk kayıp olaylarına ait veriler bankaların organizasyon yapılarına da bağlı olarak Bölüm I.4'de yer verilen alanlardan elde edilebilir.

Operasyonel risk kayıp olaylarının gerçekleşme olasılığına dair bilgiler yönetim raporları, teftiş raporları, denetim otoritesine yapılan raporlamalar ve banka dışı diğer raporlar

ile uzman görüşleri, yeniden yapılandırma planları, iş planları, bütçeler, faaliyet planları vb. kaynaklardan; operasyonel kayıpların büyüklüklerine dair bilgiler ise yöneticilerle yapılacak görüşmeler, banka içi tarihi kayıp veri tabanı, banka dışı veri tabanları vb. kaynaklardan yararlanılarak elde edilebilir. Söz konusu kaynaklardan elde edilecek bilgilerle birlikte tanımlanan riskler ve hazırlanan organizasyon haritası kullanılarak operasyonel risklerin değerlendirmesi yapılabilir ve her birimin risk profili belirlenebilir.

Geçmişe yönelik operasyonel kayıp verileri bankanın muhasebe ve kontrol, iç teftiş, bilgi teknolojileri, insan kaynakları hatta güvenlik gibi birimlerinin aralarındaki etkileşimle elde edilebilir. Bankanın faaliyetlerinde hata ve yanlışlıklar sonucu ortaya çıkan kayıplar muhasebe ve kontrol raporlarındaki kayıtlardan toplanabilir. Teftiş elemanlarının bankaların şubeleri ve genel müdürlük birimlerinde yapmış oldukları düzenli incelemeler sonucu düzenledikleri teftiş raporlarının incelenmesinden personel hataları ve dolandırıcılık olaylarına bağlı operasyonel kayıplar tespit edilebilir. Yine bankaların bilgi teknolojileri (BT) birimlerinden alınacak sistemlerdeki hataları gösteren raporlarla da mevcut sistemlerin operasyonel risklere açık zayıf yönleri belirlenebilir.

Kayıp verilerinin toplanması için bir çerçevenin ve bir takım süreçlerin oluşturulması gerekmektedir. Bu amaçla;

- Operasyonel kayıp veri tabanından Operasyonel Risk Yönetimi biriminin sorumlu olması
- Operasyonel risk verilerinin niteliğine, ne şekilde ele alınacağına ve nasıl sınıflandırılacağına dair prosedürleri açıklayan detaylı dokümantasyonun hazırlanması
- Halen operasyonel risk kayıplarının hangi Defter-i Kebir hesabına kaydedildiğinin belirlenmesi
- Operasyonel risk olaylarının kar-zararla ilişkilendirilebilmesi için Defteri Kebir hesap kodlarının oluşturulması
- Raporlama prosedürlerinin oluşturulması
- Organizasyon haritasının hazırlanması

gerekmektedir.

4. Veri Modelinin Oluşturulması

Veri modelinin oluşturulmasında halen en çok kullanılan model ER modelidir. Operasyonel risk veri modelinin oluşturulmasında da ER modeli esas alınabilir. ER modeli bir veri modelinin kurulması için gerekli yapıların listelenmesi ve tanımlanmasında kullanılırken, veri modelinin kurulması sürecinin hangi aşamalardan oluşacağına yönelik kesin standartlar bulunmamaktadır. Genellikle, ilk olarak varlıklar ve ilişkiler modellenmekte, bunu temel

nitelikler takip etmekte ve temel olmayan niteliklerin de ilave edilmesi ile model tamamlanmaktadır. ER modeline ait temel bilgilere Ek 4'de yer verilmektedir.

Operasyonel risk veri modelinin oluşturulması süreci şu aşamalardan meydana gelmelidir:

- Veri nesnelerinin ve ilişkilerin tanımlanması
- Varlıklarla ilişkilerle birlikte ilk ER diyagramının taslağının hazırlanması
- ER diyagramının sadeleştirilmesi
- Önemli niteliklerin ilave edilmesi
- Düşük önemli niteliklerin ilave edilmesi
- Genelleştirme Hiyerarşilerinin diyagramının oluşturulması
- Modelin ayrıştırma yolu ile geçerliliğinin sağlanması
- Modele risk yönetimi ile doğruluk ve bütünlüğe yönelik kuralların ilave edilmesi

Ayrıca, tasarımı gerçekleştirilen veri modelinin yanında süreçlerin tasarımı da bu aşamada gerçekleştirilmelidir. Bu kapsamda, akım şemaları, fonksiyon hiyerarşisi diyagramı, veri akım diyagramı gibi süreç modelinin unsurlarının tasarımı gerçekleştirilir.

3. Aşama- Veri Tabanının Programlanması: Mantıksal Tasarım

Veri tabanının programlanması süreci, sistemin mantıksal tasarımının gerçekleştirildiği aşamayı ifade etmektedir. Bu aşamada, bir önceki aşamada kavramsal olarak geliştirilen veri modelinin üzerine sisteme ait programlar inşa edilmektedir.

Programlama aşaması ilişkisel veri tabanı modeli kapsamında ele alındığında, kavramsal olarak geliştirilen ilişkisel tablolar üzerinde kullanıcıların istemleri doğrultusunda gerekli işlemlerin yapılabilmesi için gerekli sorgular bu aşamada tasarlanmaktadır.

Veri modeli üzerinde gerçekleştirilecek işlemler, operasyonel risk veri tabanının son kullanıcıların ihtiyaçları, risk ölçümü ve yönetimi sistemlerinin veri ihtiyacı ile veri tabanının kullanım amaçlarına göre farklılıklar gösterebilecektir. Ayrıca bu aşamada oluşturulan fonksiyon modeli, büyük oranda veri tabanına bağlanan risk ölçümü modelleri ve risk analizine yönelik diğer programlar tarafından şekillendirilmektedir.

4. Aşama- Veri Tabanının Uygulanması: Fiziksel Tasarım

Önceki aşamalarda kavramsal olarak tasarımı gerçekleştirilen veri modeli ve fonksiyon modelinin fiziksel olarak uygulamaya konulduğu aşama fiziksel tasarım aşamasıdır.

Fiziksel tasarım aşamasında, veri modeli tasarım dokümanı ile mantıksal tasarımla ilgili dokümanlardan yararlanılır. Diğer bir ifade ile mimari planı kavramsal olarak çizilen veri tabanının fiziksel olarak inşası bu aşamada gerçekleştirilir.

Bu aşamada, ilişkisel tablolar, birincil ve yabancı anahtarlar ve harekete geçiriciler fiziksel olarak tasarlanır. Ayrıca, her bir veri tabanı kullanıcısının görebileceği veri tabanı görünümü (arayüzler) de bu aşamada tasarlanır.

Bunların yanında, veri tabanının fiziki yapısı, görünümü, diğer sistemlerle bağlantıları gibi fiziki yapısına yönelik tasarımlar gerçekleştirilir.

Fiziksel tasarım aşamasında, veri tabanına aktarılacak operasyonel risk verilerinin iş kollarından ve birimlerden sisteme girişi ile veri modeli kullanılarak veri ambarına aktarılışıyla ilgili olarak daha önce tasarlanan süreçler oluşturulur.

5. Aşama- Uygulama

Uygulama aşaması, kavramsal ve fiziksel olarak tasarımı gerçekleştirilen veri tabanı sisteminin uygulamaya yönelik olarak testlerden geçirilmesi ve sistemin sürekli kullanıma açılması aşamasını ifade etmektedir.

Tasarımı tamamlanan veri tabanı sistemi, amaç ve hedeflere ulaşma seviyesi ile birlikte bankanın diğer sistemlerine uyum düzeyinin belirlenebilmesi için uygulama testlerine tabi tutulur. Uyumsuzluklarla birlikte eksiklik ve aksaklıkların belirlenmesi halinde bunların giderilmesine yönelik çalışmalar gerçekleştirilir.

Test sürecinden geçirilen veri tabanı sistemi, bankanın diğer sistemlerine entegre bir şekilde fiilen uygulamaya konulur. Bankanın risk ölçümü ve yönetimi faaliyetlerinde kullanılan sisteme veri toplama süreç ve sistemleri çalıştırılarak veri kaynaklarından sürekli veri akışı sağlanır.

Veri toplama süreci, nitelikleri belirlenen ve tanımlanan risk unsurlarına ilişkin verilerin banka içerisinde ilgili birim veya iş kollarından toplanması, banka dışında ise ilgili kuruluşlardan alınması ile başlar. Banka içinden toplanan veriler ve banka dışından elde

edilen veriler belirli filtreleme süreçlerinden geçirilerek, gruplandırılır, ardından risk ölçümü ve yönetimi amaçlarına en uygun doğru ve yeterli bilgiyi bulabilmek amacıyla analiz edilir.

Verilerin toplanmasını takiben, veriler belirli filtreleme süreçlerinden geçirilir. Gruplandırmayı takiben en anlamlı bilgiyi bulabilmek amacıyla analize tabi tutulur. İyi tasarlanmış banka içi ve dışı veri tabanlarının kullanılmasıyla, operasyonel risk birimi doğru ve isabetli analizler yapabilecek ve bankanın gelecekteki faaliyetlerine hangi risklerin zarar verebileceğini belirleyebilecek ve risk unsurlarının neden olabileceği kayıpların büyüklüğünü ve sıklığını tahmin edebilecektir.

Veri tabanındaki bilgiler, bankanın çevre faktörlerinin ve risklerinin değişeceği ve mevcut verilerin zamanla kullanışsız hale gelebileceği dikkate alınarak, düzenli olarak güncellenir.

Veri tabanı sisteminin operasyonel işlerliğinin korunması ve sürdürülmesi için gerekli bakım, koruma ve yenileme faaliyetleri de uygulama sürecinin bir parçası olarak yerine getirilmelidir.

DEĞERLENDİRME VE SONUÇ

Operasyonel riskin ölçülebilmesi ve yönetilebilmesi için belirli niteliklere sahip risk verilerinin bulunması öncelikli konuların başında gelmektedir. Risk verilerinin toplanması, analize uygun hale getirilebilmesi ve risk ölçümü ve yönetimi sürecinde sistematik bir şekilde kullanılabilmesi için bir veri tabanı sisteminin bulunması gereklidir.

Operasyonel risk veri tabanı, tüm iş kollarından ve faaliyetlerinden birbirinden farklı birçok operasyonel risk verisi topluyor olması nedeniyle kapsamı ve süreç içerisinde yer alan birimler itibariyle en kapsamlı veri tabanı sistemlerinden birisini oluşturmaktadır. Veri tabanı sisteminin kapsamı nedeniyle sistemin oluşturulmasına ilişkin faaliyetlerin de dikkatli bir şekilde belirlenmesi gereklidir.

Bankaların operasyonel risk veri tabanının oluşturulması, veri tabanı sistemi ister banka içerisinde geliştirilsin isterse de dışarıdan satın alınsın, tüm unsurlarıyla birlikte bir bütün olarak ve bunu gerçekleştirmek için gerekli faaliyetler de bir proje olarak ele alınmalıdır.

Proje, planlama ve gereksinim analizi ile başlayan, birbirini takip eden veya birbiriyle eş zamanlı olarak gerçekleştirilen faaliyetlerden oluşmalıdır. Projenin her aşaması önceden planlanmalı, çıkması muhtemel sorunların ne şekilde ele alınacağı ve nasıl çözümlenebileceğine dair eylem planları da projeye dahil edilmelidir.

Operasyonel risk veri tabanının oluşturulması, bankanın tamamında yoğun bir şekilde kaynak ve teknoloji kullanımını gerektirmektedir. Projenin kapsamının geniş olması ve kaynak ihtiyacının fazlalığı operasyonel risk veri tabanının oluşturulması sürecinin banka yönetimi tarafından sahiplenilmesini ve ilgili tüm birimlerin gerekli katkılarda bulunmasını gerektirmektedir.

Operasyonel risk yönetiminin bankanın tamamında gerek iş kolları gerekse de bankanın bütünü itibariyle gerçekleştirilmesi zorunluluğu, operasyonel risk veri tabanının da bu faaliyetleri destekleyebilecek kapsam ve kapasitede olmasını zorunlu hale getirmektedir. Bu zorunluluk veri tabanının oluşturulması ve idame ettirilmesinde banka yönetiminin rolünü ön plana çıkarmaktadır.

Operasyonel risk veri tabanının etkinliğini ve projenin başarısını etkileyen etkenlerin başında veri tabanının oluşturulmasının yanında, idame ettirilmesi ve bankanın faaliyetleri esnasında yürütülen risk yönetimi faaliyetlerinde aktif olarak kullanılması için banka içinde

gerekli oluşumların ve süreçlerin tasarlanması gelmektedir. Bu nedenle, risk yönetim sisteminin tasarımı kapsamında veri tabanına ilişkin yetki ve sorumlulukların belirlenmesi gerekmektedir.

Ayrıca, operasyonel risk verileri ve veri tabanı nedeniyle karşılaşılabilecek sorunların belirlenmesi veri tabanının işlerliğini etkileyen önemli etkenlerden bir diğerini oluşturmaktadır[9].

Bu çerçevede, veri tabanının oluşturulması bankanın operasyonel risk yönetim sisteminin diğer unsurlarından bağımsız olarak ele alınmamalı, risk yönetim sisteminin diğer unsurları ile ilişkisi her aşama göz önünde bulundurulmalıdır.

[9] Türk bankacılık sisteminde operasyonel risk veri tabanının oluşturulmasına; bu konudaki görev ve sorumluluk yapısına; ortaya çıkabilecek sorunlara ve bunların nasıl çözümlenebileceğine ilişkin önerilere yer verilen çalışma için bakınız: Mazıbaş (2006).

KAYNAKLAR

[1] Basel Committee on Banking Supervision (1998): **"Operational Risk Management"**, BIS, Basel, Switzerland, January 2001.

[2] Basel Committee on Banking Supervision (2001a): **"Operational Risk",** Supporting Document to the New Basel Capital Accord, BIS, Basel, Switzerland, January 2001.

[3] Basel Committee on Banking Supervision (2001b): **"The New Basel Capital Accord",** Consultative Document, BIS, Basel, Switzerland, January 2001.

[4] Basel Committee on Banking Supervision (2001c): **"Working Paper on the Regulatory Treatment of Operational Risk"**, BIS, Basel, Switzerland, September 2001.

[5] Basel Committee on Banking Supervision (2003): **"The Basel Capital Accord, Consultative Document",** BIS, Basel, Switzerland, July 2003.

[6] Basel Committee on Banking Supervision (2004) "**International Convergence of Capital Measurement and Capital Standarts"**, BIS, Basel, Switzerland, June 2004.

[7] Basel Committee on Banking Supervision (2005) "**International Convergence of Capital Measurement and Capital Standarts: a Revised Framework"**, BIS, Basel, Switzerland, November 2005.

[8] Baud, N., Frachot A., Rocalli T. (2002): **"Internal Data, External Data and Consortium Data for Operational Risk Measurement: How to Pool Data Properly?",** Groupe de Recherche Operationnelle, Credit Lyonnais, France.

[9] Batini, C., S. Ceri, S. Kant, and B. Navathe (1991) *Conceptual Database Design: An Entity Relational Approach,* The Benjamin/Cummings Publishing Company.

[10] British Bankers Association (2002) "**BBA Operational Risk Database Loss Categorisation**", www.bba.org.uk.

[11] Date, C. J. (1990) *An Introduction to Database Systems*, 5th ed. Addison-Wesley.

[12] Fleming, Candace C. and Barbara von Halle (1989) *Handbook of Relational Database Design*, Addison-Wesley.

[13] Fujii, Kenji (2003): **"Combining Internal Loss Data, Scorecards and Scenario Analysis",** Presentation for RMG Conference, May 30.

[14] Khan, Ali Samad (2001): **"Data Modeling"**, Presentation in *How to Master and Quantify Operational Risk, The GARP Operational Risk Seminar*, 18-19 October 2001, London.

[15] Kroenke, David (1983) *Database Processing*, 2nd ed. Science Research Associates.

[16] Mazıbaş, Murat (2002): **"Operasyonel Risklerin Stokastik Yöntemlerle Modellenmesi",** Basılmamış BDDK Uzmanlık Tezi, Eylül 2002.

[17] Mazıbaş, Murat (2003): **"Operasyonel Risk Yönetimi ve Türk Bankacılık Sistemi",** İktisat/İşletme ve Finans Dergisi, Şubat 2003.

[18] Mazıbaş, Murat (2005a): **"Operasyonel Riskin Aktüeryal Matematik Modellerle Ölçümü"**, 4. İstatistik Kongresi Bildiriler Kitabı, Antalya.

[19] Mazıbaş, Murat (2005b): **"Operasyonel Risk Ölçümü: Kayıp Dağılımları Modellemesi"**, VII. Ulusal Ekonometri ve İstatistik Sempozyumu Bildiriler Kitabı, İstanbul.

[20] Mazıbaş, Murat (2005c): **"Operasyonel Riske Basel Yaklaşımı: Üç Yapısal Blok Çerçevesinde Bir Değerlendirme",** BDDK Araştırma Raporu, 2005/1.

[21] Mazıbaş, Murat (2005d): **"Operasyonel Riske Basel Yaklaşımı: Risk Verilerine İlişkin Bir Değerlendirme",** BDDK Araştırma Raporu, 2005/2.

[22] Mazıbaş, Murat (2005e): **"Türk Bankacılık Sektöründe Operasyonel Risklerin Stokastik Yöntemlerle Ölçülmesi",** Basılmamış Gazi Üniv. SBE Ekonometri Y.Lisans Tezi, Eylül 2005.

[23] Mazıbaş, Murat (2006): **"Bankalarda Operasyonel Risk Veri Tabanının Oluşturulması",** BDDK Çalışma Raporu, 2006/3.

[24] Moffitt, Kevin, Jan van de Lagemaat, Gerrit (2003): **"Internal Loss Data Collection in an Global Banking Organisation",** Presentation, www.newyorkfed.org, May.

[25] Opel, Andy (2004). *Databases Demystified*, McGraw-Hill.

[26] Reingruber, Michael C. and William W. Gregory (1994). *The Data Modeling Handbook: A Best-Practice Approach to Building Quality Data Models*. John Wiley & Sons, Inc.

[27] Risk Yönetim Sistemleri ve Uygulama Esasları Çalışma Grubu, Operasyonel Risk Alt Çalışma Grubu (2004): **"Operasyonel Risk Veri Tabanı",** Türkiye Bankalar Birliği, Nisan 2004.

[28] Simsion, Graeme (1994). *Data Modeling Essentials*. *Analysis, Design, and Innovation,* International Thompson Computer Press.

[29] Teory, Toby J. (1999) *Database Modeling & Design: The Basic Principles*, 3rd edition, Morgan Kaufmann Publishers, Inc.

[30] Ullman, J.D., Widom, J.D. (2001). *A First Course in Database Systems,* 2nd edition, Prentice Hall.

EKLER

Ek 1: Operasyonel Risk Kayıp Olayı Sınıflandırması

Tablo 1: Operasyonel Risk Kayıp Olayları Sınıflandırması

OLAY TİPİ SINIFLANDIRMASI (1.Seviye)	TANIM	OLAY TİPİ SINIFLANDIRMASI (2.Seviye)	FAALİYET ÖRNEKLERİ (3.Seviye)
BANKA İÇİ HİLE ve DOLANDIRICILIK	**Banka içinden** en az bir tarafın işin içine karıştığı ve söz konusu taraf veya tarafların dolandırıcılık; zimmetine geçirme; düzenlemeleri, kanunları ya da şirket politikalarını dolanma veya ayrımcılık olayları şeklindeki faaliyetleri sonucu ortaya çıkan kaybı ifade eder.	***Yetkisiz İşlem***	Raporlanmayan işlemler (kasıtlı)
			Yetkisiz işlem tipi (mali kayba neden olan)
			Yanlış belirlenen pozisyonlar (kasıtlı)
		Hırsızlık ve hile, dolandırıcılık olayları	Hile ve dolandırıcılık/ kredi dolandırıcılığı/ değersiz mevduatlar
			Hırsızlık/ şantaj/ zimmetine geçirme/ soygun
			Varlıkları kişisel kullanımına alma, zimmetine geçirme
			Varlıkların kötü niyetli olarak tahribi
			Sahtekârlık
			Çek sahtekârlığı
			Kaçakçılık
			Hesabı ele geçirmek/ taklit etmek/ vb.
			Vergi kaçırmak / vergiden kaçınmak (kasıtlı)
			Rüşvet vermek veya almak / bir ücret ya da komisyon üzerinden başkasına pay vermek
			İçerden alınan bilgilerle ticaret (bankanın hesabına olmayan)
BANKA DIŞI HİLE ve DOLANDIRICILIK	**Üçüncü kişilerin** dolandırıcılık, zimmetine geçirmek ya da kanunları dolanmak şeklindeki faaliyetleri sonucu ortaya çıkan kaybı ifade eder.	***Hırsızlık ve hile, dolandırıcılık olayları***	Hırsızlık / Soygun
			Sahtekârlık
			Çek sahtekârlığı
		Sistem Güvenliği	Hacking zararı
			Bilgi hırsızlığı (mali kayıpla sonuçlanan)
İSTİHDAM UYGULAMALARI VE İŞYERİ GÜVENLİĞİ	İstihdam, sağlık veya iş güvenliği yasaları yada sözleşmelerine aykırı davranışlar, şahsi tazminat davaları ya da farklılık ve ayrımcılık olayları nedeniyle ortaya çıkan tazminatların ödenmesi suretiyle ortaya çıkan kaybı ifade eder.	***Çalışanlarla İlişkiler***	Tazminat, ikramiye, işine son verme hususları
			Organize çalışan faaliyetleri (grev vb)
		Çevre Güvenliği	Genel yükümlülük (giriş çıkışlarda güvenlik kartlarını kullanmak, vb.)
			Çalışan sağlığı ve güvenliği ile ilgili kurallara dair olaylar
			İşçilerin tazminatları
		Farklılık ve Ayrımcılık	Tüm ayrımcılık türleri (din, dil, ırk, cinsiyet vb.)

OLAY TİPİ SINIFLANDIRMASI (1.Seviye)	TANIM	OLAY TİPİ SINIFLANDIRMASI (2.Seviye)	FAALİYET ÖRNEKLERİ (3.Seviye)
MÜŞTERİLER, ÜRÜNLER & İŞ UYGULAMALARI	Kasıtsız olarak ya da ihmal sonucu belirli müşterilere karşı profesyonel yükümlülüklerin (itimat ve uygunluk yükümlülükleri de dahil olmak üzere) yerine getirilememesi ya da ürünün yapısından veya dizaynından kaynaklanan hatalar sonucu ortaya çıkan kaybı ifade eder.	***Uygunluk, Açıklama & İtimat***	İtimadın suiistimal edilmesi / Kullanılan kılavuzlara aykırı işlemler
			Uygunluk / açıklama hususları (KYC, vb.)
			Bireysel müşteri işlemlerinin gizliliği ilkesinin ihlali
			Gizliliğin ihlali
			Agresif satışlar
			Alınacak komisyon tutarını artırmak amacıyla hesap sahibinin çıkarlarını gözetmeksizin aşırı işlemler yapmak (account churning)
			Gizli bilginin kötüye kullanılması
			Ödünç verenin yükümlülüğü
		Uygunsuz iş ya da piyasa uygulamaları	Tröstlerin teşekkül etmesine karşı düzenlemeler
			Uygunsuz ticaret/ piyasa uygulamaları
			Hileli piyasa yönlendirmesi (manipülasyonu)
			İçerden alınan bilgilerle ticaret (bankanın hesabına)
			Lisanssız faaliyette bulunmak
			Para aklanması
		Ürünlerdeki kusurlar	Ürünlerdeki kusurlar (yetkisiz, vb.)
			Model hataları
		Seçme, Sponsorluk & Riskten Korunma Limitleri	Kılavuzlardaki esaslara göre müşterinin araştırılması işleminin yerine getirilmemesi
			Müşterinin riskten korunma limitlerinin aşılması
		Danışmanlık Faaliyetleri	Danışmanlık faaliyetlerinin performansı hakkındaki uyuşmazlıklar
FİZİKİ VARLIKLARA VERİLEN ZARARLAR	Doğal felaketler ya da terörizm vb. olaylar nedeniyle fiziki varlıklara verilen zararı ifade eder.	***Felaketler ve diğer olaylar***	Doğal afetlerden doğan zararlar
			Harici kaynaklardan ortaya çıkan insan kaynağı kayıpları (terörizm, kamu yada özel mülkiyete zarar verme olayları vb.)
FAALİYETİN DURMASI VE SİSTEM HATALARI	Faaliyetlerin durması, kesilmesi ya da sistem hataları sonucu ortaya çıkan kaybı ifade eder.	***Sistemler***	Donanım
			Yazılım
			Telekomünikasyon hizmetleri
			Kamu hizmetlerinin durması / kesilmesi

OLAY TİPİ SINIFLANDIRMASI (1.Seviye)	TANIM	OLAY TİPİ SINIFLANDIRMASI (2.Seviye)	FAALİYET ÖRNEKLERİ (3.Seviye)
İCRA, TESLİMAT & SÜREÇ YÖNETİMİ	Başarısız süreçler ya da başarısız süreç yönetimi ile ticari muhataplarla ve satıcılarla ilişkiler sonucu ortaya çıkan kaybı ifade eder.	***İşlemlere İlişkin Bilgilerin Tutulması, İşlemlerin Gerçekleştirilmesi & İşlem Bilgilerinin Muhafazası***	İletişimin sağlanamaması
			Bilgi girilmesi, bilgi muhafazası ya da bilgi yükleme hatası
			Son tarih ya da sorumlu bilgisi eksikliği
			Modelin ya da sistemin yanlış çalıştırılması
			Muhasebe hatası / varlık niteleme hatası
			Diğer görevlerin yerine getirilememesi
			Teslimatta hata ve başarısızlık
			Teminat yönetiminde hatalar ve başarısızlıklar
			Referans Bilgi Muhafazası
		İzleme ve Raporlama	Zorunlu raporlama yükümlülüklerinin yerine getirilememesi
			Hatalı dış rapor (kayba neden olan)
		Müşterinin Çekilmesi ve Belgelendirme	Kayıp müşteri izinleri / haklarından feragat edenlere ait bilgiler
			Yasal dokumanın kaybı ya da eksikliği
		Müşteri Hesaplarının Yönetimi	Hesaplara onaysız girişler
			Yanlış müşteri kayıtları (kayba neden olan)
			İhmal sonucu müşteri varlıklarına zarar verilmesi ya da zarar ortaya çıkması
		Ticari Muhataplar (counterparties)	Müşterilerin dışında kalan muhatapların edimlerini yerine getirmemeleri
			Müşterilerin dışında kalan muhtelif muhataplarla ortaya çıkan uyuşmazlıklar
		Satıcılar & Hizmet Sağlayıcılar	Harici hizmet sağlama
			Satıcı uyuşmazlıkları

Kaynak: BCBS (2004: s.224-225).

Ek 2: İş Kolları ve Faaliyet Sınıflandırması

Tablo 2: İş Kolları ve Faaliyet Sınıflandırması

1. SEVİYE	*2. SEVİYE*	*FAALİYET GRUPLARI*
KURUMSAL FİNANSMAN	***Kurumsal finansman***	*Birleşme ve satın almalar, aracılık yüklenimi işlemleri (underwriting), özelleştirmeler, menkul kıymetleştirmeler, araştırma, borç (merkezi hükümet, yüksek getiri), hisse senedi, sendikasyonlar, birincil halka arzlar (IPO)*
	Merkezi hükümetin / yerel yönetimlerin finansmanı	
	Tacir (merchant) bankacılık	
	Danışmanlık hizmetleri	
ALIM-SATIM & SATIŞ	***Satışlar***	*Sabit getirili, hisse senedi, döviz, ticari mal, kredi, fonlama, kendi pozisyonlarına ilişkin menkul kıymetler, ödünç ve repo işlemleri, brokerlik, borç, birincil brokerlik*
	Piyasa yapıcılığı	
	Bankaya ait hususi (proprietary) pozisyonlar	
	Hazine	
PERAKENDE BANKACILIK	***Perakende bankacılık***	*Perakende krediler ve mevduatlar, bankacılık hizmetleri, emanet (trust) ve menkul mal*
	Bireysel bankacılık	*Bireysel kredi ve mevduatlar, bankacılık hizmetleri, emanet ve menkul mal saklama, yatırım danışmalığı*
	Kart hizmetleri	*Tacir (merchant)/ticari/kurumsal kartlar, perakende*
TİCARİ BANKACILIK	***Ticari bankacılık***	*Proje finansmanı, gayrimenkul, ihracat finansmanı, ticari finansman, faktöring, finansal kiralama, kredilendirme, garantiler, ödeme emirleri*[10]
ÖDEME VE TAKAS	***Harici müşteriler***	*Ödeme ve Tahsilâtlar, fon transferleri, mahsuplaşma ve takas*
ACENTELİK HİZMETLERİ	***Muhafaza***	*Escrow, ADR*[11] *(depository receipts), menkul kıymet ödünçleri (müşteriler), kurumsal faaliyetler*
	Ticari mümessillik	*İhraç ve ödeme temsilciliği*
	Ticari muhafaza	
AKTİF YÖNETİMİ	***İsteğe bağlı fon yönetimi***[12]	*Bir havuzda toplanmış, ayrıştırılmış, perakende, kurumsal, kapalı, açık, özel hisse senedi.*

[10] Ticari bir işlemde bir tarafın diğer taraftan belli bir tutarı üçüncü bir kişiye ödeme emrini içeren bir ödeme aracını ifade eder ve üçüncü kişi genellikle birinci kişidir. Uluslararası işlemlerde "bill of exchange" olarak adlandırılmaktadır.

[11] Genellikle yabancı şirketlerin ABD bankalarında tutulan pay senetlerinin fiziki bir yer değiştirme olmaksızın banka emanetinde tutulurken satın alındığına dair makbuz.

[12] Fon sahibi ile fon yöneticisi arasındaki anlaşmaya bağlı olarak fon yöneticisine fon sahibinin talimatı olmaksızın da yatırım kararı ve pozisyon almasına imkan tanıyan bir hizmet şekli.

1. SEVİYE	*2. SEVİYE*	*FAALİYET GRUPLARI*
	İsteğe bağlı olmayan fon yönetimi[13]	*Bir havuzda toplanmış, ayrıştırılmış, perakende, kurumsal, kapalı, açık.*
PERAKENDE BROKERLİK	***Perakende brokerlik***	*İşletme ve tam hizmet*

Kaynak: BCBS (2004: s.221).

[13] Fon sahibi ile fon yöneticisi arasındaki anlaşmaya bağlı olarak fon yöneticisine ancak fon sahibinin talimatı ile işlem yapma imkanı tanıyan bir hizmet şekli.

Ek 3: Operasyonel Riskin Nedenleri Esas Alınarak Sınıflandırılması

Operasyonel riskin Basel Komitesince benimsenen tanımda da yer alan nedenleri itibariyle sınıflandırılması aşağıda yer almaktadır. Tabloda yer verilen sınıflandırma düzeylerinden ilki en genel sınıflandırma olan süreç, insan, sistem ve harici etkenlerden kaynaklanan dört ana risk grubunu ifade etmektedir. İkinci seviye sınıflandırma ise her bir ana grubun altında yer alan daha detaylı sınıfları göstermektedir. Ayrıca, ikinci seviye sınıflandırma faaliyet örnekleri de dahil edilmek suretiyle daha da detaylandırılmıştır.

Tablo 3: Operasyonel Riskin Nedensellik Sınıflaması

OPERASYONEL RİSKLER		
1. SEVİYE	**2.SEVİYE**	**FAALİYET ÖRNEKLERİ**
SÜREÇLERDEN KAYNAKLANAN RİSKLER	**Ödeme / Mutabakat, Takas Riski**	Banka içi ödeme ve takas işlemlerinde ortaya çıkan kusur, hata ve noksanlıklar
		Fiyatlandırma konusunda uzlaşılamamasından kaynaklanan zarar
		Tahvil ve senetlerin teslimatında yaşanan hatalar
		Limit aşımları
		İşlemlerin hacmi nedeniyle personelin ve sistemlerin kapasitesinin yetersiz kalması
		Diğer
	Dokümantasyon ya da Sözleşme Riski	Belgelerin uygun ve yeterli bir şekilde doldurulmaması
		Yetersiz ifadeler ve yetersiz sözleşme hükümleri
		Uygunsuz sözleşme hükümleri
		Yetersiz faaliyet kayıtları
		Müşteri bilgilerinin doğruluğunun teyidinde ve müşteriyi değerlendirmede yapılan hata ve kusurlar
		Diğer
	Değerleme/ Fiyatlandırma Riski	Kullanılan modelden kaynaklanan riskler, (uygunsuz parametreler, yanlış programlama, geçersiz varsayımlar, matematiksel hatalar vb. modele özgü riskler)
		Girdi sorunları ve hataları, veri problemleri
		Diğer
	Banka içi/ Banka dışı Raporlama Riski	Yetersiz istisnai olay raporlaması
		Muhasebeleştirme ve kayıt hataları, yetersiz ve eksik veriler
		Eksik ve yetersiz risk yönetimi raporlaması
		Eksik ve yetersiz düzenleme otoritesi raporlaması
		Eksik ve yetersiz finansal raporlama

OPERASYONEL RİSKLER		
1. SEVİYE	**2.SEVİYE**	**FAALİYET ÖRNEKLERİ**
		Eksik ve yetersiz vergilendirme raporlaması
		Eksik ve yetersiz hisse senedi ve tahvil piyasası raporlamaları
		Hesap ve kayıt düzeni hususundaki yasal düzenlemelere uygun hareket edilmemesi
		Diğer
	Kural ve Prosedürlere Uyum Riski	Banka içi kural ve prosedürlere uygun hareket edilmemesi
		Banka dışı düzenleme, kural ve prosedürlere uygun hareket edilmemesi
	Proje Riski Yönetimi ve Değişim Yönetimi	Eksik ve yetersiz proje önerisi/ planı
		Yeni ürün süreçlerinde eksiklik ve yetersizlikler
		Projeler için belirlenen maliyet ve zaman limitlerinin aşılması
		Diğer
	Satış Riskleri	Uygunsuz ürün seçimi
		Ürünün anlaşılmazlığı ve karmaşıklığı
		Eksik veya yanlış danışmanlık hizmeti (menkul kıymetleri de içeren)
		Diğer
İNSANLARDAN KAYNAKLANAN RİSKLER	**Çalışan Sahtekarlığı / Dolandırıcılığı/ Kötü Niyetli davranışı (kriminal)**	Hile ve bu konuda yapılmış gizli anlaşmalar (birden çok kişiden oluşan ve en az birinin Banka çalışanı olduğu)
		Zimmete geçirme
		Bankanın itibarının kırılmasına yönelik kasıtlı söz ve eylem
		Kasıtlı kara para aklanması
		Fiziki hırsızlık
		Fikri mülkiyete yönelik hırsızlık
		Programlama dolandırıcılığı (kasıtlı virüs bulaştırma vb.)
		Diğer
	Yetkisiz İşlem / Hileli Alım-Satım / Çalışan kabahati	Gizli ve imtiyazlı bilgilerin kötüye kullanımı
		Müşterinin çıkarlarını gözetmeden broker tarafından komisyon tutarını artırmak amaçlı aşırı alım-satım yapılması
		Piyasanın manipüle edilmesi

OPERASYONEL RİSKLER		
1. SEVİYE	**2.SEVİYE**	**FAALİYET ÖRNEKLERİ**
		Kasıtlı yanlış fiyatlandırmaya yol açan faaliyet
		Yetkisi bulunmayan muhatapla işlem yapmak
		Yetki verilmemiş ürün üzerine işlem yapmak
		Limit aşımları
		Kasıtlı yanlış modeller (modelin unsurlarının kasıtlı olarak değiştirilmesi vb. suretiyle modelin etkilenmesi)
		Alım-satım kurallarına aykırı ve bunların haricinde kalan işlemler
		Kanunsuz/ saldırgan satış taktikleri
		Prosedürlerin görmezden gelinmesi/dolanılması (kasıtlı)
		Diğer
	İstihdam Yasası	Haksız olarak personelin işine son verilmesi
		Çalışanlar arasında ayrımcılık yapılması, çalışanlara eşit fırsat verilmemesi
		Cinsel taciz vb. olaylar
		İstihdam ve ilgili diğer yasa ve düzenlemelere uygun hareket edilmemesi
		Çalışan Sağlığı ve İşyeri Güvenliği konusundaki yasa ve düzenlemelere uygun hareket edilmemesi
		Diğer
	İşgücü Kaybı	Toplu çalışan eylemleri (grev, işi yavaşlatma vb.)
		Diğer
	Kritik önemdeki personelin bulunmaması ya da kaybı	Bir iş için uygun personelin banka içinde veya banka dışında bulunamaması
		Kilit önemdeki personelin kaybı
		Diğer
SİSTEMLERDEN KAYNAKLANAN RİSKLER	**Teknoloji Yatırımı Riski**	Banka faaliyetleriyle ve mevcut sistemlerle uyumsuz teknoloji mimarisi
		Stratejik risk (platform/ hizmet sağlayıcılar)
		Faaliyet ihtiyaç ve gereklerinin yanlış veya eksik tanımlanması
		Mevcut sistemlerle uyumsuzluk
		Teknolojik donanımların eskimesi
		Yazılımların eskimesi
		Diğer

OPERASYONEL RİSKLER		
1. SEVİYE	**2.SEVİYE**	**FAALİYET ÖRNEKLERİ**
	Sistem Geliştirme ve Uygulama Riski	Eksik ve yetersiz proje yönetimi
		Projelerin maliyet/ zaman aşımları
		Programlama kusurları (banka içi ve dışı)
		Mevcut sistemlere entegre edilme veya mevcut sistemlerden ayrıştırma hataları
		Sistemin faaliyet gereklerini karşılayamaması
		Diğer
	Sistemlerin Kapasitesi	Yeterli yazılımın bulunmaması (yazılım eksikliği)
		Yeterli kapasite planlamasının bulunmaması (planlama eksikliği)
		Diğer
	Sistem Hataları	Ağ hatası
		Birbirine bağlılık (karşılıklı bağımlılık-interdependency) riski
		Bağlantı ve ara yüz hataları
		Sistem donanımında ortaya çıkan hatalar
		Yazılım hataları
		Banka içi haberleşme hataları
		Diğer
	Sistem Güvenliğinin İhlali	Banka dışından sistem güvenliği ihlalleri
		Banka içi sistem güvenliği ihlalleri
		Programlama dolandırıcılığı
		Bilgisayar virüsleri
		Diğer
HARİCİ (DIŞSAL) ETKENLERDEN KAYNAKLANAN RİSKLER	**Yasal ve Toplumsal Sorumluluk**	Çevrenin korunması uygulamalarının ihlali
		İtimat ve güvenin ihlali, aracılık görevinin yerine getirilmemesi (emanette saklanması işlemlerinde vb.)
		Yasaların ve mevzuatın yanlış yorumlanması
		Yanlış betimleme (tanımlama)
		Diğer
	Kriminal Faaliyetler	Banka dışı dolandırıcılık, çek dolandırıcılığı, sahtekârlık (sahte imza vb.)
		Müşteri tarafından hileli hesap açılması
		Müşterinin kendisi hakkında gerçeği yansıtmayan

OPERASYONEL RİSKLER		
1. SEVİYE	**2.SEVİYE**	**FAALİYET ÖRNEKLERİ**
		yanlış bilgi vermesi
		Şantaj
		Soygunlar (hırsızlık dahil)
		Kara para aklanması
		Terörizm, bombalı saldırı
		Sabotaj, toplumsal hareketler vb. nedenlerle faaliyetlerin durması
		Mülkiyete fiziki zarar verilmesi
		Kundaklama
		Diğer
	Harici Hizmet Sağlama (outsourcing) / Tedarikçi Riski	Hizmet sağlayıcının iflas etmesi
		Hizmet sağlayıcının sorumluluklarını yerine getirememesi (gizli bilgilerin kötüye kullanımı gibi)
		Eksik ve yetersiz sözleşme
		Hizmet sağlama anlaşmasına aykırı hareket edilmesi
		Hizmet sağlayıcının teslimatı gerçekleştirmemesi
		Hizmet sağlayıcıların verdiği hizmetlerin iyi icra edilememesi
		Diğer
	Banka İçi Hizmet Sağlama (Insourcing) Riski	Banka içi hizmet sağlamada sorun yaşanması
		Diğer
	Felaketler ve Altyapı hizmetlerinin kesilmesi	Yangın
		Sel
		Deprem
		Diğer doğal (jeolojik, meteorolojik) afetler
		Toplumsal felaketler (kimyasal serpinti, çarpışma vb.)
		Ulaşım sorunları
		Enerji sorunları
		Harici iletişim sorunları
		Su kesintileri
		Bina ve çalışma alanı bulunmaması
		Diğer

OPERASYONEL RİSKLER		
1. SEVİYE	**2.SEVİYE**	**FAALİYET ÖRNEKLERİ**
	Düzenleyici Otorite Riski, Politik Risk	Düzenleme otoritesinin mevzuatı değiştirmesi
		Savaş
		Kamulaştırmalar
		Faaliyet engellemeleri
		Vergi rejiminin değiştirilmesi
		Diğer kanunlarda değişiklikler
		Siyasi İstikrarsızlık
		Diğer

Kaynak: British Bankers Association (BBA).

Ek 4: ER Modellerine İlişkin Temel Kavramlar

ER modelinin veri nesneleriyle ilgili temel yapı unsurları varlıklar, nitelikler ve ilişkilerden oluşmaktadır. Bunlara ilişkin rehber niteliğindeki açıklamalar bölümler itibariyle aşağıda verilmektedir:

a. Varlıklar (entities)
b. Nitelikler (attributes)
   - Geçerliliğini gösteren nitelikler
   - Türetilen nitelikler ve Kod değerleri
c. İlişkiler (relationships)
d. Veri nesnelerinin isimlendirilmesi
e. Nesne tanımı
f. Tasarım belgesine bilgilerin kaydedilmesi

A. Varlıklar

ER modelinde kullanılan ve sanal dünyadaki bir varlığı ifade eden "varlık" (entity) kavramı konusunda farklı tanımlar bulunmaktadır:

- *"Hakkında bilgi saklanan diğerlerinden ayırt edilebilir kişi, yer, şey, olay veya kavram"* (Bruc)
- *"Ayırt edilebilir şekilde belirlenen şey"* (Chen)
- *"Veri tabanında temsil edilecek herhangi ayırt edilebilir nesne"* (Date)
- *"...hakkında bilgi sakladığımız herhangi bir şey (örneğin tedarikçi, makina ekipmanı, çalışan, uçak koltuğu, vb) . Her bir varlık çeşidi için belirli nitelikler saklanmaktadır"* (Martin)

Yukarıda yer alan tanımlar varlık konusunda ortak noktalar içermektedir:

- Bir "varlık", bir "*şey*", "*kavram*" veya "*nesne*"dir. Bununla birlikte, varlıklar bazen iki veya daha çok nesne arasındaki ilişkileri temsil edebilirler. Bu türdeki bir varlık "*yardımcı varlık (associative entity)"* olarak bilinmektedir.
- Varlıklar betimleyici bilgi içeren nesnelerdir. Belirlenen bir veri nesnesi diğer nesnelerce betimleniyorsa, bu bir varlıktır. Bu parça ile ilişkilendirilmiş herhangi bir betimleyici bilgi mevcut değilse, bu bir varlık değildir. Bir veri nesnesinin varlık olup olmadığı kuruluşlara veya modellenen faaliyete bağlı olacaktır.
- Bir varlık özellikleri paylaşılan birçok şeyi temsil etmektedir. Bunlar yalnız başlarına "*şeyler*" değildir. Örneğin "sistemlerdeki hatalar" ile "sistemlerin yetersizliği"

olayları, operasyonel risk olayı olma, sistemlerden kaynaklanma, bilgi sistemlerinde ortaya çıkma gibi birçok ortak niteliği paylaşmaktadır. Burada "sistemlerin yetersizliği" ile "sistem hataları" veri modeli için birer varlıktır.

- Ortak özellikleri paylaşan varlıklar genelleştirme hiyerarşilerine dönüştürülmeye adaylardır.
- Varlıklar zaman noktaları arasındaki ayrıştırmalarda kullanılmamalıdır. Örneğin, birinci çeyrekteki brüt kar, ikinci çeyrekteki brüt kar vb. şeklinde değil, "brüt kar" olarak birleştirilmelidir. Zamana göre sınıflandırmayı yapmak için zaman aralığını gösteren bir niteleyici kullanılabilir.
- Kullanıcıların hakkında bilgi elde etmek istedikleri her şey bir varlık olmayacaktır. Birden çok varlığı içeren bir karmaşık kavram bunu temsil edebilir.

B. Nitelikler

Nitelikler, varlıkları tanımlayan veya betimleyen veri nesneleridir. Varlıkları tanımlayan nitelikler *"temel nitelikler (key-attributes)"* olarak adlandırılmaktadır. Varlıkları betimleyen nitelikler ise *"temel olmayan nitelikler (non-key attributes)"* olarak adlandırılmaktadır.

Niteliklerin tanımlanması süreci de varlıklarla benzerlikler taşımaktadır. Nitelikler konusunda betimleyici bir takım isimlerin ele alınması gerekmektedir:

1. Niteliklerin Geçerliliğinin Sağlanması:

Nitelik değerleri yalnızca tek bir gerçeği temsil etmelidir *(atomic*). Kümelenmemiş veriler kullanmak daha basit programlama yapmayı, verinin tekrar tekrar kullanabilmeyi, değişiklerin daha kolay işlenebilmesini sağlamaktadır. *Ayrıştırma (normalization)* işlemi takip edilen *"tek bir gerçek"* kuralına bağlı bulunmaktadır.

Bu kurala ilişkin genel aykırılıklar basit kümeleme (toplama), karmaşık kodlar, metin blokları, karıştırılmış ana alanlar gibi durumlarda ortaya çıkmaktadır.

2. Türetilmiş Nitelikler ve Kod Değerleri:

Veri modelleme uzmanları türetilmiş nitelikler ve değerleri kodlardan oluşan niteliklerin veri modelinde yer alıp almaması konusunda aynı fikirde değildirler.

Türetilmiş nitelikler bir formül tarafından veya diğer niteliklerin üzerine bir toplama işlemi ile yaratılmış niteliklerdir. Türetilmiş verilere yönelik eleştiriler, türetilmiş niteliklerin veri tabanında saklanmaması gerektiği ve dolayısıyla veri modeline dahil edilmemesine ilişkin öneriye dayanmaktadır. Bu önerinin lehindeki görüşlere göre,

- Türetilmiş veri genellikle yöneticiler ve kullanıcılar için önemli olduğundan veri modeline dahil edilmemelidir.
- Türetilmiş niteliklerin yazılı hale getirilmesi diğer nitelikler kadar belki onlardan daha çok önemlidir.
- Veri modelinde türetilmiş niteliklere yer vermek bunların nasıl uygulanacağını ima etmemektedir.

Kodlanmış bir değer bir gerçeği temsil etmek için bir veya birden çok harf veya rakam kullanmaktadır. Örneğin, "cinsiyet" değeri "Erkek" ve "Kadın" dan ziyade "E" ve "K" harflerini kullanacaktır. Bu uygulamaya karşı olanlar genellikle kodların son kullanıcılar için anlaşılabilir anlamları olmadığı ve verinin işlenmesindeki karmaşıklığı daha da arttığını ifade etmektedir. Lehinde olanlar ise, bir çok kuruluşun uzun yıllardır kodlanmış niteleyici kullandıkları, bu kodların alandan tasarruf sağladığı ve esneklik sağladığını iddia etmektedirler.

C. İlişkiler

İlişkiler, varlıklar arasındaki bağlantıları göstermektedir. Genellikle, iki veya daha çok varlığı birbirine bağlayan bir yüklem ile gösterilmektedir. Örneğin,

"*Çalışanlar projede* ***görevlendirilirler.***"

İlişkilerin belirlenmesi esnasında, bunlar kardinalite, seçeneklilik, yön ve bağımlılık açısından sınıflandırılmalıdır. İlişkilerin tanımlanması neticesinde bazı ilişkiler dikkate alınmayacak ve bazı yeni ilişkiler ilave edilebilecektir. Kardinalite, varlıklar arasındaki ilişkileri bir varlığın kaç durumunun bir diğer varlığın bir durumu ile ilişkili olduğunun ölçülmesi yoluyla sayısallaştırılır. Kardinalite belirleyebilmek için, öncelikle varlıklardan birisinin bir durumunun mevcut olduğu varsayılır. Bunun ardından, ikinci varlığın ilk varlığın bu durumu ile ilişkili kaç spesifik durumu olduğu belirlenir. Bu analiz varlıkların yerleri değiştirilerek tekrarlanır. Örneğin,

"Çalışanlar aynı anda üçten çok olmamak üzere projede ***görevlendirilebilirle****r, her bir projede görevlendirilmiş en az iki çalışan bulunmaktadır."*

Burada, çalışanlardan-projeye doğru olan ilişkinin kardinalitesi üçtür. Projelerden-çalışanlara doğru olan ilişkinin kardinalitesi ise ikidir. Dolayısıyla ilişki "çoklu ilişki" olarak adlandırılır.

Bir ilişkinin kardinalitesi sıfır ise bu ilişki "seçenekli" bir ilişkidir. Eğer ilişkinin en az bir kardinalitesi bulunması gerekiyorsa, ilişki "zorunlu" ilişkidir. Seçenekli ilişkiler genellikle koşullu ifadelerle gösterilmektedir. Örneğin,

"*Bir çalışan bir projede **görevlendirilebilir**.*"

Diğer taraftan, zorunlu ilişkiler ise zorunluluk ifade eden bir sözcükle ifade edilir. Örneğin,

"*Bir öğrenci her dönem en az üç derse kaydolmak **zorundadır**.*"

D. Veri Nesnelerinin İsimlendirilmesi

Veri nesnelerine verilecek isimler tek (unique), son kullanıcı için anlamlı olmalı ve nesneyi tek ve doğru bir şekilde betimleyebilmek için gerekli en az kelimeden oluşmalıdır.

Varlıklar ve niteliklere verilecek isimler tekil isimler iken ilişki isimleri genellikle yüklemlerden oluşmaktadır.

Özellikle büyük veri tabanlarının geliştirilmesi esnasında, farklı birimlerin aynı veri nesnesini ifade etmek için farklı isimler kullanabileceği göz önünde bulundurularak varlıklar ve nitelikler için aynı anlama gelen isimlerin (synonyms) belirlenmesinde ve ayırt edilmesinde dikkatli olunması gerekmektedir.

E. Nesne Tanımı

Veri modellemesiyle ilgili tüm tarafların hangi nesnelerin hangi kavramları temsil ettiğini tam olarak bilebilmeleri için tam ve doğru tanımlama çok önemlidir. Tanımlar kullanıcıya aşina terimler içermeli ve nesnenin neyi temsil ettiği ve kuruluşta hangi rolü oynadığı konusunu tam olarak açıklamalıdır. Bazı yazarlar son kullanıcıların yaptığı tanımlamaların kullanılmasını önermektedir.

Nesnelerin tanımlanması esnasında, bir varlığın iki farklı kavramı temsil ettiğini (homonyms) veya iki farklı varlığın aynı şeyi temsil ettiğini (synonyms) durumların ayırt edilmesinde dikkatli olunmalıdır. Bu durum özellikle, kişilerin veya kuruluşların bir olay ya da süreç hakkında kendi fonksiyonları açısından düşünmelerinden kaynaklanmaktadır. Örneğin, risk yönetimi birimi "kayıp" kavramını risk yönetimi bakış açısıyla ele alırken, finansal raporlama ve muhasebe birimi ise "kayıp" kavramını muhasebe anlamında finansal zarar olarak ele alabilecektir. Dolayısıyla, aradaki farklılıkların düzeltilmesi gerekmektedir.

F. Tasarım Belgesine Bilgilerin Kaydedilmesi

Tasarım belgesinde modelde kullanılan tüm nesnelerle ilgili detaylı bilgiler kaydedilmektedir. Modelleme sürecinde nesneler isimlendirildiklerinde, tanımlandıklarında ve betimlendiklerinde bu bilgiler tasarım belgesine işlenmelidir. Modellemede otomatik bir tasarım aracı kullanılmıyorsa, tasarım dokümanı kâğıt üzerine veya kelime işlemcisine

kaydedilmelidir. Bu belgenin organizasyonu konusunda herhangi bir standart bulunmamakla birlikte belge isimler, tanımlar ve nitelikler için etki alanları (domainler) hakkında bilgiler içermelidir.

Tasarım belgesine ilişkin olarak IDEF1X modelleme yönteminde kullanılan Varlık-Varlık matrisi ile Varlık-Nitelik matrisinin kullanılması nesnelere ait bilgilerin tutulmasında faydalı olabilecektir.

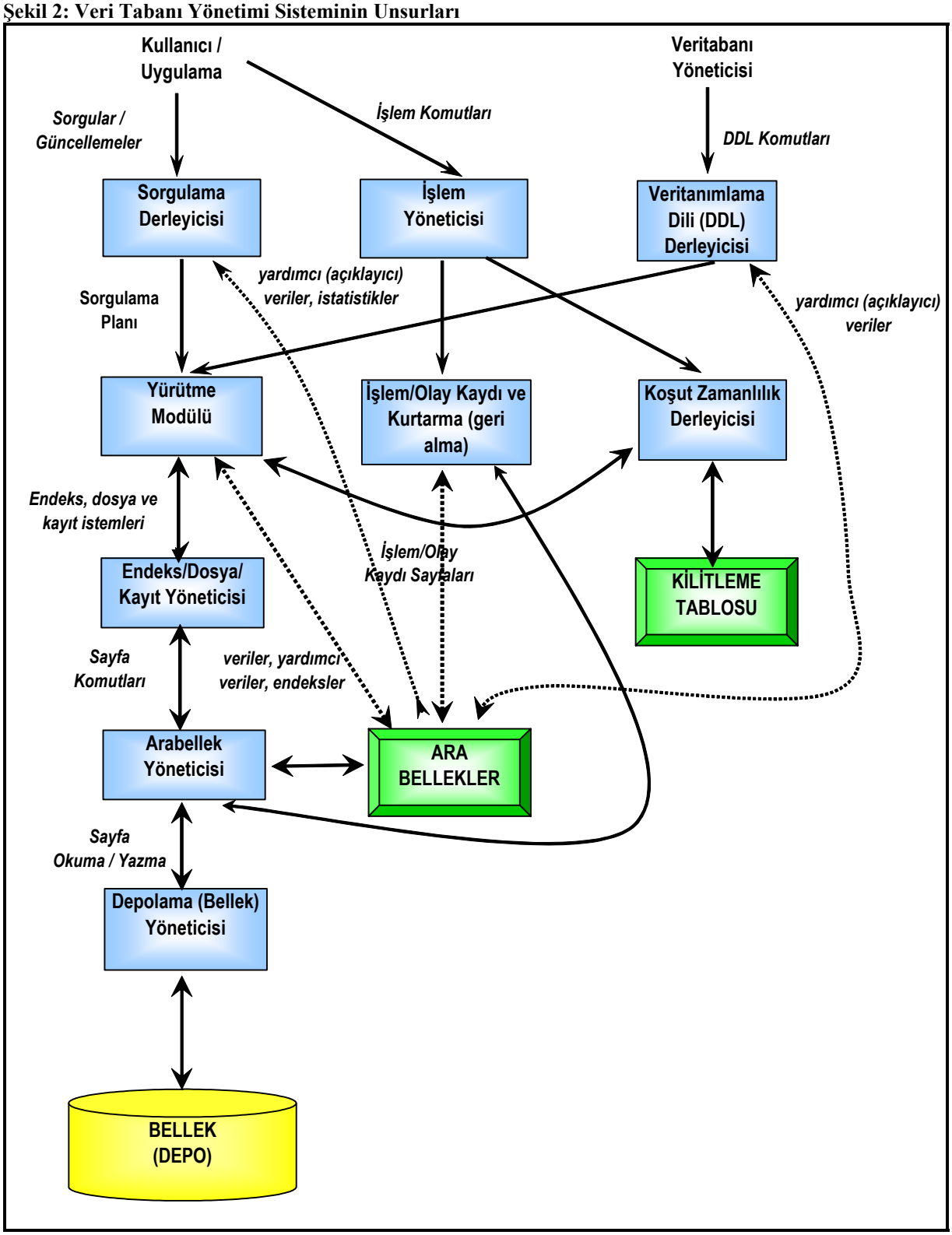
Varlık-Varlık matrisi, varlıklar arasındaki ilişkileri gösteren iki boyutlu bir matristir. Belirlenmiş tüm varlıkların isimleri her iki eksen üzerine de kaydedilerek, varlıklar arasındaki ilişki ilk belirlendiğinde iki varlığın kesişimi olan hücre "X" işareti işaretlenir. Ardından, ilişkinin detayı belirlendiğinde ise ilişkinin detayını ve kardinalitesini gösteren notasyonla değiştirilir.

Varlık-Nitelik matrisi ise her bir niteliğin varlıklara ne şekilde atandığını göstermektedir. Format olarak Varlık-Varlık matrisi ile aynıdır. Ancak, Varlık-Nitelik matrisinde nitelik isimleri satırlarda, varlık isimleri ise sütunlara kaydedilir.

Ek 5: Veri Tabanı Sistemlerinin Unsurları ve İşleyişleri

Bir veri tabanı sisteminin temel unsurları ve işleyiş yapısı aşağıda özetlenmektedir:

Şekil 2: Veri Tabanı Yönetimi Sisteminin Unsurları



Kaynak: Ullman, Widom (2001).

BDDK
BANKACILIK
DÜZENLEME VE DENETLEME
KURUMU

Atatürk Bulvarı No:191 06680 Kavaklıdere / ANKARA
Tel :(0312) 455 65 29 Fax: (0312) 424 17 42
www.bddk.org.tr