

**ISO 27001 STANDARDI KAPSAMINDA KURUMSAL BİLGİ GÜVENLİĞİ  
VE İŞLETME PERFORMANSI ARASINDAKİ İLİŐKİ: BİST 100  
ENDEKSİNDE YER ALAN İŐLETMELER ÜZERİNE BİR UYGULAMA**  
**RELATIONSHIP BETWEEN CORPORATE INFORMATION SECURITY AND  
COMPANY PERFORMANCE IN THE SCOPE OF ISO 27001 STANDARD:  
AN APPLICATION ON COMPANIES IN THE BIST 100 INDEX**

**Őerife ÖNDER**

Dumlupınar Üniversitesi, Sosyal Bilimler Meslek Yüksekokulu, KÜTAHYA  
(serife.onder@dpu.edu.tr)

**ÖZ**

Hem kamu hem de özel işletmeler açısından bilginin oluşturulması ne kadar önemli ise, oluşturulan bilgilerin güvenli bir şekilde saklanması da en az onun kadar önemli bir konudur. ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı, kurumsal bilgi güvenliğinin sağlanmasına yönelik olarak geliştirilen standarttır.

Bu çalışmada bilgi güvenliğinin işletmelerde bir uygulaması olan ISO 27001 sertifikasının varlığı ile şirket performansı arasında istatistiksel olarak anlamlı bir ilişki bulunup bulunmadığı analiz edilecektir. Yapılan analizde BIST 100 endeksinde yer alan işletmeler örneklem olarak belirlenmiştir. Çalışmada Lojistik Regresyon Modeli kullanılarak veriler SPSS16 programında analiz edilecektir. Analiz sonucunda ISO 27001 sertifikasına sahip olmanın, işletme performansını olumlu yönde etkilemesi beklenmektedir.

**Anahtar Sözcükler:** Kurumsal bilgi güvenliği, ISO 27001, BİST 100 endeksi, İşletme performansı

**ABSTRACT**

*The importance of the creation of information in terms of both public and private company is a matter of at least as important as the safekeeping of the information generated The ISO 27001 Information Security Management System (ISMS) standard is a standard developed to provide enterprise information security.*

*In this study, it will be analyzed whether there is a statistically significant relationship between the presence of ISO 27001 certification, which is an implementation of information security in companies, and performance. In the analysis, companies included in the BIST 100 index are determined as the sample. The data will be analyzed at SPSS 16 program using Logistic Regression Model. As a result of the analysis, it is expected that having ISO 27001 certificate will affect the performance of companies positively.*

**Keywords:** Enterprise information security, ISO 27001, BIST 100 index, Company performance

## 1. Giriş

Bilgi, *Türk Dil Kurumu tarafından "İnsan aklının erebileceği olgu, gerçek ve ilkelerin bütünü, bili, malumat"* veya *"İnsan zekâsının çalışması sonucu ortaya çıkan düşünce ürünü, malumat, vukuf"* şeklinde tanımlanmıştır (TDK). Günümüzde her alanda en önemli kavramlardan biridir bilgi, hatta önemini ifade etmek için, içinde yaşadığımız çağ bile bilgi çağı olarak adlandırılır. Artık maddi ve manevi değerlerin yanına, bilginin değeri de eklenmiştir. Çünkü bilginin değeri arttıkça, sahip olduktan sonra sağladığı güçte artmaktadır. Bu nedenle sadece devletler ve toplum için değil tüm kurumlar ve hatta bireyler içinde bilgi değerli ve önemlidir (Evrin & Demirer,2011:25) .

Kurumlar *açısından* bilgi, artan önemi nedeniyle, en önemli üretim faktörü olarak kabul edilmektedir. Çünkü kurumların rekabet üstünlüğünü sağlayabilmeleri için almaları gereken kararlarda bilginin sistematik bir şekilde oluşturulması, sürekli olarak yenilenmesi, depolanması, paylaşılması ve kullanılması gerekmektedir. Yani bilginin yönetilmesi gerekmektedir (Uzun & Durna,2008:33). Bilginin üretilmesinden kullanılmasına kadar olan her aşamada ise, bilginin korunması ve güvenliğinin sağlanması gerekir.

Olası tehditlere karşı bilgi güvenliğinin sağlanmasına yönelik uygulamalar, Uluslararası Standardizasyon Örgütü (ISO) tarafından standartlar ile belirlenmiştir. Ayrıca ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı olarak belgelendirilmektedir. Günümüzde işletmeler kurum imajı ve saygınlığı, rekabet avantajı gibi farklı nedenlerle ISO'nun yayınlamış olduğu standartları belgelendirmek için ciddi paralar harcamaktadır. Bu ve buna benzer çalışmaların odak noktası ise, işletmelerin ISO standardizasyon belgelendirmeleri için katlanmış olduğu maliyetlerin, işletmeye finansal olarak geri dönüşünün söz konusu olup olmadığıdır?

Bu çalışmada ISO 27001 Bilgi Güvenliği Yönetim Sistemi (BGYS) standardı ile işletmelerde kurumsal bilgi güvenliğinin sağlanmasının, işletmelerin finansal verilerine etkisinin bulunup bulunmadığı İkili Lojistik Regresyon Analizi ile tespit edilecektir.

## 2. Bilgi Güvenliği ve ISO 27001 Belgesi

Bilgi güvenliği, bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sağlanması olarak tanımlanmaktadır. Buna göre (Doğantimur,2009:7);

- *Gizlilik*, bilginin yetkisi olmayan kişiler tarafından erişilememesidir,
- *Bütünlük*, bilginin içeriğinin değiştirilmeden ya da silinmeden doğruluğunun ve tamlığının korunmasıdır,
- *Erişilebilirlik*, bilgiye erişim yetkisi olan kişiler tarafından istenildiği anda ulaşılabilir olmasıdır.

Bilginin değeri bu üç temel unsurun birlikte sağlanmasıyla mümkündür. Dolayısıyla bilginin gizliliğinin sağlanması erişilebilirliğini engellememelidir. Ya da bilgiye erişim sağlanıyor ancak bütünlüğünü sağlanamıyor ise, yanlış ve eksik bilgi olacaktır. Bilgi güvenliği, bilginin bir varlık olarak ele alınması, yetkisiz erişim ve kullanım, yok etme, değiştirme, bozma gibi saldırı tehditlerinden verilerin korunması sürecidir (Baykara vd.,2013:238).

Bilgi güvenliğinin sağlanması ihtiyacı bilgisayar ve iletişim teknolojilerinde yaşanan hızlı gelişmeler nedeniyle artmıştır. Ayrıca elektronik uygulamaların artması, bilgilerin ağ üzerinden paylaşılması, bilgiye her noktadan erişilmesi ve bu ortamlarda oluşan açıkların çok büyük tehdit

oluřturması gibi sebepler nedeniyle bilgi gvenliđinin sađlanması gerekir (Vural & Sađırođlu, 2008:507).

Kurumsal bilgi gvenliđi, kurumların bilgi varlıklarının tespit edilmesini, zafiyetlerinin belirlenmesini, oluřabilecek tehdit ve tehlikelerden korunması iin gvenlik analizlerinin yapılmasını ve nlemlerin alınmasını iermektedir (Dođantimur,2009:8). Kurumsal bilginin gvenliđinin sađlanması iin mevcut yazılımlar, donanımlar, ortamlar ve insan kaynakları kullanılmaktadır. Ayrıca kurumsal bilgi gvenliđi devamlılık gerektiren bir sretir ve bu sre kurumsal bilgi gvenliđi standartları erevesinde ynetilmelidir (Vural & Sađırođlu,2008:508). Bilgi Gvenliđi Ynetim Sistemi (BGYS) genel olarak, kuruma ait bilgilerin ynetilmesi amacıyla benimsenmiř olan sistematik yaklařım Őeklinde tanımlanmaktadır (Marttin & Pehlivan,2009:50). İlk olarak İngilizler tarafından 1995 yılında BS 7799 bilgi gvenliđi ynetimi standardı geliřtirilmiřtir. Bu standart daha sonra BS 7799-1 ve 7799-2 olarak yayınlanmıřtır. Ancak İngiliz standardı olan bu standartlar uluslararası standart niteliđinde deđildi (Glmř,2010:59). Uluslararası standartlar, eřitli standardizasyon komitelerindeki uluslararası uzmanların ortak tecrbelerinden ve bilgilerinden oluřturulmaktadır. En nemli ve yaygın olarak kullanılan uluslararası standartlar, ISO ve Uluslararası Elektroteknik Komisyonu (IEC) komiteleri tarafından yapılır (Anttila vd.,2012:425). Bilgi gvenliđi standardı olan BS 7799-2 standardı ISO tarafından revize edilerek ISO/IEC 27001:2005 olarak deđiřtirilmiř ve yrrlđe girmiřtir. Bu standart, kurumların bilgi gvenliđi ynetim sistemini kurmaları iin gereklilikleri kapsamaktadır (Glmř,2010:59).

ISO 27001 Bilgi Gvenliđi Ynetim Sistemleri – Gereklilikler (Gereksinimler) Standardı kurumsal bilgi gvenliđinin bir kurumda nasıl uygulanabileceđini aıklayan standarttır. Bu standart ile kurumda Bilgi Gvenliđi Ynetim Sisteminin kurulması, gerekleřtirilmesi, iřletilmesi, izlenmesi, gzden geirilmesi, srdrlmesi ve iyileřtirilmesi sađlanmaktadır (Dođantimur,2009:12). ISO/IEC 27001 standardı teknik bir standart deđildir. Bu standart, iřletmelerin bilgi gvenliđi iin gerekli olan faaliyetlerini ortaya koyar fakat bunların nasıl gerekleřtirilebileceđini iřletmeye bırakır. BGYS'nin ISO tarafından belirlenen teknik Őartlarını sađlayan, BGYS iin gerekli iř ve planlama Őemalarını hazırlayan, BGYS dngs gerekleřtirilen iřletmelerin belgelendirmesinde "ISO/IEC 27001:2005 Bilgi Gvenliđi Ynetim Sistemleri-Gereksinimler" standardı kullanılmaktadır (Yılmaz, 2014:51-52).

Bilgi gvenliđi ynetim sistemi ISO 27001 standardının iřletmelere sađlayacađı faydaları Őu Őekilde zetlemek mmkndr (Park vd.,2010:12, Baykara vd., 2010:60);

- Mevcut bilgi sisteminde oluřabilecek olası tehditlerden kaynaklanan potansiyel kayıpların ngrlmesi,
- Kurum varlıklarının istikrarının, etkinliđinin ve gvenliđinin arttırılması,
- Risk analizi ve deđerlendirilmesi ile etkin bir risk ynetiminin sađlanması,
- Yksek riskli alanların belirlenerek gvenlik nlemlerinin alınması,
- iřletme paydařları ve ortakları iin kurumsal saygınlıđın korunması,
- iřletmenin kurumsal hedeflerini desteklemesi,
- Kuruma rekabet avantajı sađlaması,
- Kurum imajına olumlu etki sađlaması olarak sayılabilir.

Tüm bu faydalar ISO 27001'in işletmelerde verimliliği ve etkinliği sağlamasına böylece de maliyetlerin düşmesine ve işletme karlılığının artmasına neden olmaktadır. Bu durum işletme performansını olumlu yönde etkilemekte ve işletmeye rekabet avantajı sağlamaktadır.

### 3. Literatür

Literatürde kurumsal bilgi güvenliği uygulamalarının göstergesi olarak ISO 27001 sertifikasını temel alan ve finansal göstergeler ile ilişkisini inceleyen bazı çalışmalara bu başlık altında yer verilmiştir. Ancak işletmelerin 27001 sertifikasyonu ile finansal performansı arasındaki ilişkiyi inceleyen çalışmalar çok sınırlıdır.

Park vd. (2010) Güney Kore'de ISO 27001 belgesine sahip olan 76 işletmeye gönderdikleri anket formları neticesinde elde etmiş oldukları verileri regresyon analizi ile incelemişlerdir. Gönderilen 76 anketten geriye dönüş sağlanan 34 anketin sonuçlarına göre ISO 27001 standartının işletmenin toplum nezdinde kurumsal itibarını arttırarak satışları etkilediği sonucuna ulaşmışlardır.

Alber & Nabil (2015) Mısır'daki 32 banka içerisinden 13'ü üzerinde yapmış oldukları regresyon analizi ve ki-kare testleri ile bankanın BGYS'i ile karlılığı arasındaki ilişkiyi incelemişlerdir. Bankanın karlılığını ölçmek için Aktif Karlılığı (ROA), Öz Kaynak Karlılığı (ROE) ve Sermaye Karlılığı (ROC) değişkenlerini kullanmıştır. Yapılan analizler sonucunda BGYS ile sadece ROC arasında istatistiksel olarak anlamlı bir ilişki bulunmuştur.

Hsu vd, (2016) Avrupa ve Amerika'dan toplam 25 şirket üzerinde ISO27001 ve işletme performansı arasındaki ilişkiyi incelemişlerdir. Araştırmacılar işletmelerin ISO 27001 belgesi sahip olmadan önce ve sahip olduktan sonraki dönemlerinde ROA ve hisse senedi Al-Tut (Buy and Hold) anormal getirileri arasında bir fark olup olmadığını hipotez testleri ile incelemişlerdir. Yapılan analiz sonuçlarında işletmelerin söz konusu finansal verileri ile ISO 27001 sertifikasına sahip olmaları arasında istatistiki açıdan anlamlı bir ilişki olmadığı ortaya çıkmıştır.

Türkiye'de ISO 27001 standardı ile ilgili yapılan çalışmalarda Doğan Timur (2009), Marttin & Pehlivan (2010), Evrin & Demirel (2011) çalışmalarda bilgi güvenliği, bilgi güvenliği yönetim sistemi ve süreçleri teorik olarak açıklanmaktadır. Dolayısıyla bu kapsamda işletme performansına yönelik ilişkisini inceleyen ampirik bir çalışma bulunmamaktadır.

ISO 27001 veya BGYS ile örgütsel performans üzerinde literatürde yapılan çalışmalar mevcuttur. Bu çalışmalardan Kong vd (2015), Said vd. (2013) ve Hall vd. (2011) çalışmaları örnek olarak gösterilebilir. Bu çalışmalarda uygulanan anket yöntemi ile işletmelerin örgütsel performansı üzerinde BGYS'nin etkisi ölçülmektedir. Ayrıca BGYS'nin çalışanlar üzerinde de etkileri ölçen çalışmalar mevcuttur. Bu tarz çalışmalara da Debaghi (2016) çalışması örnek olarak gösterilebilir.

Araştırmacılar ISO kalite belgeleri ile finansal performans arasındaki ilişkiyi farklı değişkenler kullanarak incelemektedir. ISO tarafından yayınlanan çok fazla kalite standardı bulunmakta ve bu alanda da oldukça farklı çalışmalar yapılmaktadır. Genellikle araştırmacılar ilgilendikleri bir alana ilişkin veriler ile analizler gerçekleştirmektedir. (Karim, 2015:33-34). Örneğin ISO 9001 Kalite Yönetim Sistemi Standardı ile finansal performans ilişkisini inceleyen literatürde oldukça fazla sayıda çalışma mevcuttur.

ISO 9001 ve iřletme performansı iliřkisine ynelik literatr incelendiđinde ok farklı sonuların bulunduđu grlmektedir. Bu sonuları finansal performansı olumlu ynde etkilediđi tespit edilen alıřmalar ile finansal performansı sınırlı dzeyde ya da nemli bir Őekilde etkilemediđi tespit edilen alıřmalar olmak zere genel olarak iki bařlık altında toplamak mmkndr (Ayrıay vd., 2009:172, İlkey ve Aslan,2012:755, Adıgzel ve Aydınlı,2016:368);

**Tablo 1.** İřletmelerde ISO 9000-9001 Kalite Ynetim Sistemi Standardının Varlıđı ile İřletme Performansı Arasındaki İliřkileri İnceleyen alıřmalar

<b>Finansal Performansı Pozitif Ynde Etkilediđi Tespit Edilen alıřmalar</b>	<b>Finansal Performansı Sınırlı Dzeyde ya da Hi Etkilemediđi Tespit Edilen alıřmalar</b>
Carr vd., (1997), Hendricks ve Singhal (1997), Erođlu (2003), Terziovski vd., (2003), Erođlu (2004), Corbett, vd., (2005), Sharma (2005), Yetiřen (2011), Gnebakan-Basık (2011), Al-Refaie- Ghnaimat- Li (2012)	Simmons ve White(1999), Lima vd.(2000), Kasapopur (2000), Singels- Ruel- Water (2001), Wayhan- Kirche- Khumawala (2002), Tsekouras- Dimara ve Skuras (2002,) Morris (2006), Aslan (2007), Costaa vd. (2009)

**Kaynak:** Ayrıay vd., 2009:172, İlkey ve Aslan,2012:755, Adıgzel ve Aydınlı,2016:368 alıřmalarından derlenmiřtir.

Tablo 1’den de grleceđi zere hem ulusal hem de uluslararası dzeyde yapılan alıřmalarda iřletmelerde ISO 9000-9001sertifikasyonu ile iřletme performansı arasında tek bir sonutan bahsetmek mmkn deđildir. Dolayısıyla da bu konuda literatrde bir grř birliđinin bulunduđunu sylemek mmkn deđildir. Trkiye’de yapılan alıřmalar genel olarak incelendiđinde arařtırma yntemi olarak anket uygulaması (Adıgzel ve Aydınlı (2016), Aslan, İlkey ve zdemir (2009), Kutlu ve Duran (2015), Erođlu (2004), İlkey ve Aslan (2012), Sarıkaya ve Altunıřık (2004)) yapıldıđı grlmektedir. Bu anket alıřmalarının ierisinde bir alt bařlık olarak finansal performans, anketi cevaplayan kiři tarafından deđerlendirilmektedir. Ancak Ayrıay vd, (2009) tarafından yapılan alıřmada, iřletmelerin ISO 9000 sertifikasının varlıđı ile finansal performans gstergeleri incelenmiřtir. Buna gre alıřmada OYAK grubuna bađlı 4 imento iřletmesinin 1998-2007 yılları arasındaki finansal performansları rasyolarla (Aktif Karlılıđı, Satıř Karlılıđı, Net Kar Marjı, SMM/Net Satıřlar, (SMM+Faaliyet Giderleri) / Net Satıřlar ve satıřlardaki Byme) hesaplanmıřtır. Bylece iřletmelerin bu sertifikaya sahip olmadan nce ve sonraki performansları karřılařtırılmıřtır. Sonu olarak rneklemde yer alan 4 iřletmeden ikisinin finansal performansı zerinde olumlu bir etki tespit edilirken, diđer iki iřletmede herhangi bir olumlu etki oluřturmadıđı tespit edilmiřtir.

Hem ISO 9001 standardı hem de ISO 27001 standardı, ynetim sistemlerinin srekli iyileřtirilmesi ile ilgili ynetimsel kavramlara dayanmaktadır. Ayrıca ikisinin de sertifikasyon yaklařımları neredeyse birbiriyile aynıdır. Ancak ISO 9001 standardı akademik alıřmalarda en ok kabul gren standartlardan biridir. Dolayısıyla ISO 27001 standardı ile ilgili yapılan alıřmalarda ISO 9001 standardı literatrnden faydalanılmaktadır (Hsu, vd.,2016:4843). Bu alıřmada da yukarıda anlatılan literatr erevesinde model, deđiřken ve veri seimi gerekleřtirilmiřtir.

#### **4. Arařtırmanın Modeli ve rneklemleri**

Bu alıřma Borsa İstanbul (BİST) 100 Endeksinde iřlem gren iřletmelerin kurumsal bilgi gvenliđi faaliyetleri zerinde iřletmenin finansal yapısının etkisini test etmeyi amalamıřtır. Bunun iin BİST 100’de iřlem gren 100 iřletme rneklem olarak alınmıřtır. Fakat bu rneklem

içerisinden 9 işletmenin finansal verilerine ulaşamadığı için örneklem dışında bırakılmıştır. Örneklem dışında kalan işletmelerden sonra toplam örneklem sayısı 91 işletme olarak gerçekleşmiştir. Örneklemde yer alan işletmelerin internet sitelerinde, Kamuyu Aydınlatma Platformunda yapmış oldukları yıllık faaliyet raporlarından işletmelere ilişkin finansal bilgiler alınmıştır.

Çalışmada işletmelerin kurumsal bilgi güvenliği faaliyetleri ISO 27001 Bilgi Güvenliği Yönetim Sertifikası sahibi olmaları ile ölçülmektedir. 2016 yılı için ISO 27001 sertifikasına sahip 39 işletme BIST 100'de faaliyette bulunmaktadır. ISO 27001 belgesi bulunan işletmeler 1 olmayan işletmeler 0 olarak kodlanıp veri seti oluşturulmuştur. Bu nedenle araştırmanın analiz yöntemi olarak İkili Lojistik Regresyon Analizi seçilmiştir.

Çalışmada kurumsal bilgi güvenliği faaliyetlerine etki eden finansal değişkenler için işletmelerin karlılığı (Aktif Karlılık Oranı- ROA ve Özsermaye Karlılık Oranı-ROE), kaldıraç oranı ve şirket büyüklüğü değişkenleri seçilmiştir. Bu değişkenleri kullanarak oluşturulan model Eşitlik 1'de gösterilmektedir.

$$ISO27001 = \beta_0 + \beta_1 ROE + \beta_2 ROA + \beta_3 SIZE + \beta_4 LEV + \varepsilon \quad (1)$$

Kullanılan bu model Chua, Goh ve Wan (2003)'ün çalışmasında finansal performans göstergeleri olarak tanımlanan değişkenleri temel alınarak yeniden formüle edilmiştir. Bu model ilgili alanda yapılan çalışmalarda kullanılan genel kabul görmüş değişkenleri içeren bir modeldir. Bu çalışmada, İkili Lojistik Regresyon Modeli kullanılarak veriler SPSS15 programında analiz edilmiştir.

Bu eşitlikte modelin bağımlı değişkeni olan "ISO27001" ISO 27001 sertifikasını, " $\beta_0$ " modelin sabit terimini, " $\beta_1, \beta_2, \beta_3$ , ve " $\beta_4$ " bağımsız değişkenlerin parametre katsayılarını, " $\varepsilon$ " modelin hata terimini göstermektedir. " $LEV$ " modelin bağımsız değişkenlerinden kaldıraç oranı değişkenini, " $SIZE$ " işletme büyüklüğünü, " $ROA$ " aktif karlılık oranını " $ROE$ " ise özsermaye karlılık oranını göstermektedir<sup>1</sup>.

$ISO27001$  değişkeni BIST100'de yer alan işletmelerin belgesine sahip olup olmadıklarına göre ölçülecektir. belgesine sahip olan işletmeler için 1, yer olmayanlar için 0 değeri kullanılacaktır.

$SIZE$  değişkeni işletme büyüklüğünü temsil etmektedir. İşletme büyüklüğü değişkeni işletmelerin toplam varlıkları (Aktif) TL cinsinden tutarı ile hesaplanacaktır.

$LEV$  değişkeni işletmelerin kaldıraç oranı ile hesaplanmaktadır. Bu değişken toplam borçların toplam varlıklara bölünmesi ile hesaplanmaktadır.

$ROA$  değişkeni işletmelerin aktif karlılık oranını göstermektedir. Bu değişken net karın aktif toplamına bölünmesi ile hesaplanmaktadır.

$ROE$  değişkeni özsermaye karlılığını göstermektedir. Bu değişken net karın özsermaye bölünmesi ile hesaplanmaktadır.

1 Değişkenler arasında dağılım marjını normalize etmek için bütün değişkenler modelde doğal logaritma alınarak kullanılmıştır.

## 5. Bulgular

Eřitlik 1’de kurumsal bilgi güvenliđinin iřletme performansına etkisini ölçmek üzere kurulan modelde yer alan deđişkenlere iliřkin tanımlayıcı istatistikler Tablo 1’de gösterilmektedir.

**Tablo 1.** Modele İliřkin Tanımlayıcı İstatistikler

Deđişkenler	N	En Düşük	En Yüksek	Ortalama	Standart Sapma
ISO27001	91	0	1	0,429	0,497
SIZE	91	19,494	26,465	22,228	0,498
LEV	91	-5,033	0,121	-0,716	0,733
ROE	91	-1,215	0,732	0,065	0,272
ROA	91	-0,0001	2,573	0,513	0,655

Eřitlik 1’de yer alan deđişkenlerden *ISO27001* deđişkeni sıfır ila bir arasında deđer almaktadır. *SIZE* deđişkeni ise 19,494 ile 26,465 arasında deđer alırken ortalama olarak 22,228 deđerine ulaşmaktadır. *LEV* deđişkeninin dalgalanma marjı daha düşüktür. -5,033 ila 0,121 arasında deđişen deđerler almaktadır. *ROA* ve *ROE* deđişkenleri karlılık oranlarını gösteren deđişkenlerdir. Bunların dalgalanma marjı mevcut deđişkenler içerisinde en düşük olanıdır.

**Tablo 2.** Hosmer ve Lemeshow Testi

Ki-Kare	Serbestlik Derecesi	Önem Düzeyi
5,455	8	0,708

Eřitlik 1’de yer alan modelin analizine geçmeden önce, istikrar ve uyum kořulları arařtırılmalıdır. Söz konusu modelin uyum iyiliđini test etmek için Hosmer ve Lemeshow testi kullanılmıřtır. Tablo 2’de yer alan sonuçlara göre Hosmer ve Lemeshow Ki-Kare deđeri 5,455’dir. Bu deđer 0,05 istatistiki önem düzeyinde anlamlı bulunmamıřtır. Bu söz konusu modelin verilere yeterli ve iyi bir řekilde uyduđunu ifade etmektedir.

**Tablo 3.** Model Katsayılarına İliřkin Omnibus Testi

Adım		Ki-Kare	Serbestlik Derecesi	Önem Düzeyi
1	Adım	11,623	4	0,020
	Blok	11,623	4	0,020
	Model	11,623	4	0,020

Lojistik regresyon analizinde modelin uyumunu ve yeterliliđini inceleyen bir diđer test Omnibus testidir. Tablo 3’te Omnibus testi Ki-Kare deđeri 11,623 olduđu ve serbestlik derecesi 4 için istatistiki önem düzeyinin 0,020 olduđu görülmektedir. Tablo 3’te ortaya konan bu sonuç, sadece sabitin yer aldıđı model ile bađımsız deđişkenlerin yer aldıđı model arasında fark olmadıđına iliřkin hipotezi ret edilerek, bađımlı deđişken ile modelde yer alan bađımsız deđişkenlerin arasındaki iliřkinin varlıđını ortaya koymaktadır.

**Tablo 4.** Sınıflandırma Tablosu

		Beklenen Durum		
Gerçek / Gözlenen Durum		ISO27001 Belgesine Sahip Olmama	ISO27001 Belgesine Sahip Olma	Doğru Sınıflandırma Yüzdesi
Adım 1	ISO27001 Belgesine Sahip Olmayanlar	40	12	76,9
	ISO27001 Belgesine Sahip Olanlar	20	19	48,7
Doğru Toplam Sınıflandırma Yüzdesi				64,8

İki kategoriden oluşan bağımlı değişkeni açıklamak için kategorilerin gerçek duruma ne kadar iyi uyduğu Tablo 4'teki sınıflandırma tablosu ile gösterilmektedir. Tablo 4'te ISO 27001 belgesine sahip olmayan 62 işletmeden 40'ının doğru olarak sınıflandırıldığı ve doğru sınıflandırma yüzdesinin %76,9 olduğu görülmektedir. Bu oran ISO 27001 belgesine sahip olan işletmelerin yüksek bir oranda doğru olarak sınıflandırıldığını ifade etmektedir. ISO27001 belgesine sahip olan 39 işletmenin ise 19 tanesi doğru sınıflandırılarak doğru sınıflandırma yüzdesinin %48,7 olarak gerçekleştiği görülmektedir. Bu oran ISO 27001 belgesine sahip olan işletmelerin doğru sınıflandırma yüzdesinin yarı yarıya olduğunu ifade etmektedir. Toplam sınıflandırma yüzdesi ise %64,8 olarak gerçekleşerek model veri uyumunun orta seviyede iyi olduğu görülmektedir. Toplam sınıflandırma yüzdesi, ISO27001 belgesine sahip olan firmaların sınıflandırma yüzdesinin nispeten düşük olmasından dolayı bu seviyede gerçekleşmiştir.

**Tablo 5.** Modelin Özeti

Adım 1	-2 LogLikelihood	Cox&Snell R Kare	Nagelkerke R Kare
	112,666	0,120	0,161

Çoklu regresyon modellerinin analizindeki  $R^2$  değerlerinin benzeri olarak ikili lojistik regresyon modellerinde Cox&Snell  $R^2$  ve Nagelkerke  $R^2$  değerleri bulunmaktadır. Bu iki  $R^2$  değerinin yorumlanmasında Nagelkerke  $R^2$  değeri çoklu regresyon analizlerinde düzeltilmiş  $R^2$  değerine benzemektedir. Tablo 5'teki  $R^2$  değerleri incelendiğinde işletmelerin kurumsal güvenlik faaliyetlerine finansal verilerinin etkisini ölçen bu modelde yer alan bağımsız değişkenlerin, bağımlı değişkeni açıklama yüzdesi %16,1 seviyesinde kaldığı görülmektedir. Söz konusu oran düşük olmakla birlikte ilişkinin varlığını da ifade etmektedir.

**Tablo 6.** Modelin Analizi Sonucunda Değişkenlerin Katsayıları

	B	Standart Hata	Wald	Serbestlik Derecesi	Önem Düzeyi	Exp(B)
ROE	2,218	1,098	4,080	1	0,043*	9,189
ROA	-0,807	0,615	1,723	1	0,189	0,446
LEV	0,766	0,484	2,502	1	0,114	2,151
SIZE	-0,132	0,195	0,462	1	0,497	0,876
Sabit	3,394	4,604	0,543	1	0,461	29,776

\* %5, önem düzeyinde istatistiki açıdan anlamlı olduğunu göstermektedir.



Modelin geneline iliřkin uyum ve istikrar kořulları incelendikten sonra söz konusu modelde yer alan bağımsız deęişkenlerin anlamlılığı ve bağımlı deęişken üzerindeki etkisine geçilebilir. Tablo 6'da modelde yer alan 4 bağımsız deęişkendен haricindeki bütün deęişkenler istatistiki açıdan anlamsız çıkmıştır. Eřitlik 1'deki modelde yer alan bağımsız deęişkenlerden *ROA*, *LEV* ve *SIZE* deęişkenleri istatistiki açıdan anlamsız bulunmuştur. İřletmelerin ISO27001 belgesine sahip olarak gerçekleřtirmiş oldukları kurumsal bilgi güvenliği faaliyetleri üzerinde sadece deęişkeni etkilidir. ROE deęişkeni % 5 istatistiki önem düzeyinde anlamlı bulunmuştur. deęişkeninin katsayısının yorumlanmasında Exp(B) katsayısı yorumlanacaktır. Çünkü Exp(B) katsayıları "B" orijinal beta katsayılarının logaritmik dönüşüme tabi tutulmuş deęeridir. Buna göre istatistiki açıdan anlamlı çıkan deęişkeninde meydana gelen 1 birimlik artış yönünde deęişim, iřletmeleri ISO27001 belgesine sahip olma ihtimalini  $[(9,189-1)*100]$  %818,9 arttırmaktadır. Bu oran oldukça yüksek bir düzeye iřaret etmektedir.

## 6. Sonuç

ISO tarafından pek çok kalite standardı ve bu standartlara baęlı olarak kalite belgesi verilmektedir. İřletmelerin bu kalite belgelerini edinmeleri hem zaman ve çaba hem de maliyet unsuru içermektedir. Dolayısı ile iřletmeleri bu kalite belgelerini almaya itebilecek pozitif güdülerin ortaya çıkması gerekmektedir. Bu güdüleyiciler genellikle iřletmenin rekabet avantajı yaratıp karını arttıracığına iliřkin beklentiler olarak tanımlanmaktadır. ISO kalite belgelerinin finansal performans belirleyicileri veya ISO kalite belgelerinin finansal performans üzerindeki etkilerini ölçen çalışmalar literatürde oldukça fazladır. Bu çalışmalarda ISO kalite belgeleri ve finansal performans etkileşimi için, üzerinde uzlaşmış tek bir sonuç bulunamamıştır.

ISO'nun belirlemiş olduęu standartlardan bir tanesi de ISO 27001 standardıdır. İletişim ve bilgisayar teknolojisinde yaşanan gelişmelere baęlı olarak ortaya çıkan yeni ekonomide en önemli kavram bilgidir. Özellikle internetin yaygınlaşması ve bilgisayar teknolojilerindeki gelişmeler hem bilginin üretilmesi hem de yayılmasında oldukça önemli hale gelmiştir. Fakat bu teknolojik gelişmeler aynı zamanda üretilen bilginin korunması ve saklanmasını da zorlaştırmaktadır. Bu alanda iřletmelerin uygulaması gereken standartlar ISO tarafından 27000 ailesinin bir üyesi olan 27001 BGYS standardı ile ortaya konmuştur.

Bu çalışmada ISO 27001 standardı ile iřletmenin karlılık (ROA, ROE), kaldıraç ve iřletme büyüklüğünün ilişkisi ikili lojistik regresyon analizi ile ölçülmüştür. Söz konusu analiz sonucunda ISO 27001 standardının tek belirleyicisi kurulan model çerçevesinde öz sermaye karlılığı olduęu sonucuna ulaşılmıştır.

## Kaynakça

- Adıgüzel O. & Aydınlı C. (2016). ISO 9001 kalite yönetim sisteminin biliřim sektöründe faaliyet gösteren firmaların iřletme performansı üzerine etkileri: Ankara ili örneęi. Kastamonu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, 12: 365-383.
- Alber N. & Nabil M. (2015). The impact of information security on banks' performance in Egypt, International Journal of Economics and Finance, 7(9):219-225.
- Antila J., Jussila K., Kajawa J. & Kamaja I. (2012). Integrating ISO/IEC 27001 and other managerial discipline standards with processes of management in organization. Seventh International Conference on Availability, Reliability and Security, 425-436.
- Aslan E., İlkay M. S. & Özdemir A. İ. (2009). ISO 9001 belgeli KOBİ'lerin performans farklılıklarının bazı faktörler bakımından analizi. Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 25: 35-40.

- Ayrıçay Y., Uğurlu M. & Uğurlu Ö. Y. (2009). Kalite yönetim uygulamalarının finansal performans üzerine etkisi: Ampirik bir analiz. Muhasebe ve Finansman Dergisi (Mufad Journal), 42:169-180.
- Baykara M., Daş R. & Karadoğan İ. (2013). Bilgi güvenliği sistemlerinde kullanılan araçların incelenmesi. 1 st International Symposium on Digital Forensics and Security (ISDFS'13), 20-21 May 2013, Elazığ.
- Chua C., Chow G. M. & Wan T. B. (2003). Does ISO 9000 certification improve business performance? International Journal of Quality & Reliability Management, 20(8): 936-953.
- Dehaghi M. R. (2016). The relation of information security management system efficiency with organizational agility case study: Isfahan Mobarakeh Steel Company, International Journal of Business and Management, 11 (8):116-123.
- Doğantimur F. (2009). ISO 27001 Standardı Çerçevesinde Kurumsal Bilgi Güvenliği. Maliye Bakanlığı Strateji Geliştirme Başkanlığı, Mesleki Yeterlilik Tezi, Ankara
- Eroğlu E. (2004). Küçük ve Orta Ölçekli işletmelerdeki kalite güvence uygulamalarının bütünsel işletme performansı üzerine etkilerinin incelenmesi. Yönetim Dergisi, 15(49): 88-102.
- Evrin V. & Demirer M. (2011). Kurumsal bilgi güvenliği süreç çalışmaları: ISO/IEC-27001 örneği, IV.Ağ Ve Bilgi Güvenliği Ulusal Sempozyumu, sy: 25-33, Atılım Üniversitesi, Ankara.
- Gülmüş M. (2010). "Kurumsal Bilgi Güvenliği Yönetim Sistemleri ve Güvenliği", Yıldız Teknik Üniversitesi Fen Bilimleri Enstitüsü, İstanbul
- Hall J. H., Sarkani S. & Mazzuchi T. A. (2011), Impacts of organizational capabilities in information security, Information Management & Computer Security, 19 (3): 155-176.
- Hsu C., Wang T., & Lu A. (2016). The Impact of ISO 27001 certification on firm performance., 49th Hawaii International Conference on System Sciences, p:4842-4848.
- İlkay M. S. & Aslan E. (2012). The Effect of the ISO 9001 quality management system on the performance of SMEs, International Journal of Quality & Reliability Management, 29(7):753-778.
- Karim A. (2015). ISO certification and financial performance: a review, The Journal of Global Business Management, 11(2):32-38.
- Kong H., Jung S., Insung L. & Yeon S. J. (2015) Information security and organizational performance: empirical study of Korean securities industry, ETRI Journal, 37 (2):428-437.
- Kutlu S. & Duran C. (2015). Sanayi işletmelerinde toplam kalite yönetimi ve ISO 9000 uygulamalarının performans üzerine etkisi. Dumlupınar Üniversitesi Sosyal Bilimler Dergisi, 28:235-252.
- Marttin V. & Pehlivan İ. (2009). ISO 27001:2005 Bilgi güvenliği yönetimi standardı ve Türkiye'deki bazı kamu kuruluşu uygulamaları üzerine bir inceleme. Mühendislik Bilimleri ve Tasarım Dergisi, 1(1):49-56.
- Park C., Jang S. S. & Park Y. T. (2010). A study of effect of information security management system[ISMS] certification on organization performance. International Journal of Computer Science and Network Security, 10(3):10-21.
- Said A. R., Haslinda A., Jegak U. & Zainal A. M. (2014). Relationship between organizational characteristics and information security knowledge management implementation, Social and Behavioral Sciences 123:433 – 443.
- Sarıkaya N. & Altunışık R. (2004). Kalite iyileştirme faaliyetlerinin algılanmasının işletme performansı üzerindeki etkilerinin incelenmesi ve Türkiye uygulaması. Yöneylem Araştırması/Endüstri Mühendisliği - XXIV Ulusal Kongresi, 15-18 Haziran 2004, Gaziantep – Adana.
- TDK, Türkiye Dil Kurumu, www.tdk.gov.tr
- Uzun H. & Durna U. (2008). İşletmelerde rekabet unsuru olarak bilgi yönetimi, Niğde Üniversitesi İİBF Dergisi, 1(1): 33-40.
- Vural Y. & Sağıroğlu Ş. (2008). Kurumsal bilgi güvenliği ve standartları üzerine bir inceleme. Gazi Üniversitesi. Mühendislik ve Mimarlık Fakültesi Dergisi. 23(2): 507-522.
- Yılmaz H. (2014). TS ISO/IEC 27001 bilgi güvenliği yönetimi standardı kapsamında bilgi güvenliği yönetim sisteminin kurulması ve bilgi güvenliği risk analizi, KİDDER Kamu İç Denetçileri Derneği, 15(1):45-59.