İşletme Akademisi Dergisi
2022, 3 (2): 161-187
DOI:10.26677/TR1010.2022.1026
Dergi web sayfası: www.isakder.org

Türk Bankacılık Sektöründe İç Denetim Yoluyla Siber Güvenlik Yönetişimi

Prof. Dr. Seval Kardeş SELİMOĞLU
Anadolu Üniversitesi, İktisadi ve İdari Bilimler Fakültesi, İşletme Bölümü, Eskişehir.
sselimoğlu@anadolu.edu.tr, www.orcid.org/0000-0003-1185-9980

Dr. Mustafa Hakan SALDI
Endüstri Mühendisi, hamusaldi@hotmail.com, www.orcid.org/0000-0001-5043-4606

Öz

Makalede, iç denetim faaliyetlerinin siber güvenlik yönetişimindeki konumunun belirlenmesi hedeflenmiştir. Öncelikle kavramsal çerçeveye değinilerek, konu ile ilgili tanımlardan ve terimler arasındaki ilişkilerden bahsedilmiştir. Sonrasında ise araştırma metodu olarak kullanılan, keşifsel sıralı karma yöntemlerin nasıl kullanıldığı görsellerle ifade edilmiştir. Bu doğrultuda, delphi yöntemi, yarı yapılandırılmış görüşmeler yoluyla, açık uçlu sorular ve anketler vasıtası ile veri toplama aracı olarak kullanılarak, panelistlerin konuya ilişkin farkındalık seviyeleri ve fikir birliğine varma düzeylerinin ölçülmesi amaçlanmıştır. Katılımcılar tarafından, yasal mevzuata uyumun sağlanması, etik kuralların oluşturulması ve kurumsal yönetim ilkelerinin planlanması hususlarında siber güvenlik yönetişiminin etkili bir faktör olduğu ve bu faktörün de bilgi teknolojileri kontrollerinin yanında iç denetimin destekleyici fonksiyonlarına ihtiyaç duyduğu vurgulanmıştır. Çalışmada, özellikle, sağlıklı bir siber güvenlik yönetişiminin temin edilmesindeki temel yapı taşlarından olan gizlilik, bütünlük ve erişilebilirlik unsurlarının kusursuza yakın olarak işleyebilmesi için gerekli kurum kültürünün nasıl sağlanabileceği üzerine bir dizi fikir elde edilmiştir. Bu bağlamda, yetkilendirme sistemi üzerinde bilhassa durulmuştur.

Anahtar Kelimeler: İç Denetim, Siber Güvenlik, Yönetişim, Delphi Tekniği

Makale Gönderme Tarihi: 15. 05. 2022

Makale Kabul Tarihi: 13. 06. 2022

* Bu çalışma Prof. Dr. Seval Kardeş Selimoğlu danışmanlığında yürütülen "The Cyber Security Governance by Internal Audit in Turkish Banking Sector" başlıklı doktora tezinden türetilmiştir.

Önerilen Atıf:
Kardeş Selimoğlu, S., Saldı, M. H. (2022). Türk Bankacılık Sektöründe İç Denetim Yoluyla Siber Güvenlik Yönetişimi, *İşletme Akademisi Dergisi*, 3 (2):161-187.

Journal of Business Academy
2022, 3 (2): 161-187
DOI:10.26677/TR1010.2022.1026
Dergi web sayfası: www.isakder.org

The Cyber Security Governance by Internal Audit in the Turkish Banking Sector

Prof. Dr. Seval Kardeş SELİMOĞLU
Anadolu University, Faculty of Economics and Administrative Sciences, Eskişehir.
sselimoğlu@anadolu.edu.tr, www.orcid.org/0000-0003-1185-9980

Dr. Mustafa Hakan SALDI
Industrial Engineer, hamusaldi@hotmail.com, www.orcid.org/0000-0001-5043-4606

Abstract

The article aims to determine the position of internal audit activities in cyber security governance. First of all, the conceptual framework was mentioned, and the definitions related to the subject and the relationships between the terms were mentioned. Then, it was expressed with visuals how exploratory sequential mixed methods used as research methods were used. In this direction, the delphi method is used as a data collection tool through open-ended questions and surveys through semi-structured interviews to measure the awareness levels and consensus levels of the panelists. It was emphasized by the participants that cyber security governance is an effective factor in ensuring compliance with legal regulations, establishing ethical rules and planning corporate governance principles, and that this factor needs the supporting functions of internal audit as well as information technology controls. In particular, the study obtained a series of ideas on how to provide the necessary corporate culture for the close to perfect functioning of confidentiality, integrity and availability elements, which are the basic building blocks in ensuring a healthy cyber security governance. In this context, the authorization system has been particularly emphasized.

Keywords: Internal Audit, Cyber Security, Governance, Delphi Technique

Received: 15. 05. 2022

Accepted: 13. 06. 2022

Suggested Citation:
Kardeş Selimoğlu, S., Saldı, M. H. (2022). The Cyber Security Governance by Internal Audit in the Turkish Banking Sector, *Journal of Business Academy*, 3 (2):161-187.

1. GİRİŞ

Özellikle, bilgisayar ve iletişim kuramlarında, ürünlerinde ve uygulamalarında, son yarım asırda kat edilen mesafeye orantılı olarak tasarlanan gelişen teknoloji süreçlerinde ortaya çıkan dijitalleşme altyapısının ve çevrim içi faaliyetlerin kurumlardaki iş akışlarını doğrudan ve dolaylı yollardan etkilemesi ile siber güvenlik aktivitelerinin yönetişimi ve denetimi konusu bilimsel çevre tarafından araştırma konusu olmuştur. Bilgi teknolojilerinde meydana gelen ve sürekliliğini koruyan yenilikler iç denetimin faaliyet alanlarını ve perspektifini de etkileyerek işletme süreçlerinin veri güvenliği bazında kontrolünün nasıl ve hangi standartlara göre sağlanması gerektiği sorunsalını doğurmuştur. Bilhassa, finans sektörü kapsamında yer alan kurumlardan bankaların, depoladığı, işlediği ve transferini gerçekleştirdiği yüksek boyutlu müşteri verilerinin siber risklere karşı savunmasının sağlanarak, finansal işlemlerin güvenliğinin temin edilmesi birincil önem arz etmektedir. Bu bağlamda, iç denetim ekiplerinin geleneksel rolünün, bankaların bilgi teknolojilerindeki kontrol süreçlerinin gerçekleştirilmesinde ve kurum içi ve dışı yönetişim mekanizmasının sürdürülmesinde, nasıl bir adaptasyon dönemine girdiği sorusu da gün yüzüne çıkmaktadır. Bahsedilen nedenlerin akabinde tanımlanan araştırma konusuna ve sorunsalına yönelik yapılacak bir çalışmanın hem bilim çerçevesine hem de banka endüstrisinde faaliyet gösteren kurumlara, yöneticilere ve uzmanlara ışık tutabileceği faraziyesinden yola çıkılarak, Türkiye'deki bankaların siber güvenlik yönetişimi süreçlerinde iç denetimin nasıl bir rol üstlendiği mercek altına alınmış, analizler yapılmış ve ileriye yönelik öneriler sunulmuştur. Çalışma, bankaların karşılaşabileceği siber güvenlik açıklarını önlemelerinde, iç denetim fonksiyonlarının hangi oranda etkili olduğunu ortaya çıkarmak açısından önem taşımaktadır. Araştırmanın sorunsalı, iç denetim ekiplerinin bankacılık sektöründe siber güvenlik yönetişimi dahilindeki süreçlerde hangi konumda oldukları ve nasıl sorumluluk üstlendikleridir. Çalışmanın amacı ise, siber güvenlik yönetişiminde iç denetim faaliyetlerinin nasıl çerçevelendiğini incelemektir.

Bu doğrultuda, çalışmanın birinci yani giriş bölümünde kavramsal çerçeve dahilindeki iç denetim, siber güvenlik, yönetişim ve risk kontrolü terimleri araştırılmış ve iç denetim, yönetişim, risk ve kontrol kavramları arasındaki bağlantı incelenerek, siber güvenlik yönetimi açısından denetim faaliyetlerinin hangi yönde faaliyetler gösterebileceği üzerine varsayımlar yapılmıştır. Ardından, çalışmanın ikinci bölümünü kapsayan yöntem kısmına geçilmiş ve araştırmanın rotası belirlenmiştir. Akabinde ise çalışma kapsamındaki analizler sonucu elde edilen bulgular sunulmuştur.

Denetim işlemleri temel olarak iç ve dış olarak sınıflandırılırken, İç Denetim Enstitü'sünün resmi tanımına göre iç denetim, risk yönetimi ve yönetişim sistemlerinin verimliliklerinin ve etkinliklerinin değerlendirilmesi ve iyileştirilmesi için sistematik ve disiplinli yaklaşımların bağımsız ve objektif bir perspektifle organizasyon içi çalışanlar tarafından tasarlanmasıdır. Dış denetimde durum iç denetimden farklı olarak, organizasyon haricinden bir ekibin veya kurumun, organizasyonun denetim faaliyetlerini gerçekleştirmesidir (Gantz, 2014). Benzer biçimde, iç denetim süreçleri işletmelerin risk yönetimi sistemlerindeki yönetişim mekanizmalarının kontrolünün ve geliştirilmesinin sağlanmasında değer katıcı faaliyetlerin kurumlara entegre olmasında da fonksiyonlara sahiptir. Bunlara ilaveten, iç denetim, risk yönetiminin organizasyonel planlara ve hedeflere tutarlı bir çerçevede yapıldığına dair teminat sağlanmasında danışmanlık faaliyetlerinin yürütülmesini de kapsar. Doğal olarak, iç denetim mekanizmasının oluşturulması ve sürdürülmesi, sektörlere özgü kalite metriklerinin ve standartlarının sağlanması için uluslararası standartların ve kurumsal prensiplerin net bir biçimde anlaşıldığı profesyonellik gerektirmektedir. Özellikle bu sebep nedeniyle, iç denetim fonksiyonları disiplinli, sistematik, bağımsız ve objektif yaklaşımlarla sürdürülmelidir. Bu

bağlamda, işletmelerdeki kontrol sistemleri verimliliğin ve etkinliğin ölçülmesinde birer gösterge olarak iç denetçiler tarafından analiz edilir ve değerlendirilir (Pickett, 2011:205).

Genel çerçeveden bakıldığında, işletmelerde, iç denetimin muhasebe ve finansman süreçlerinin kontrol edilmesindeki geleneksel rolü teknoloji kullanımının zorunlu hale gelmesi ile birlikte yetersiz kalmaya başlarken, işletmelerin sahip olduğu stratejik öneme sahip varlıkların, özellikle kritik altyapılarının ve verilerinin, bilgi sistemlerindeki güvenliğinin temin edilmesi için gerekli önlem planlarının yapılarak, gizliliğinin, bütünlüğünün ve ulaşılabilirliğinin takip edilmesi zorunluluğu ortaya çıkmıştır. Konu detaylı açıdan değerlendirilecek olunursa, organizasyonlarda, bilgi sistemlerindeki kontrolün sağlanmasında, siber risklerin tespit edilerek sınıflandırılması, raporlanması ve takip edilmesi süreçlerinde de iç denetimin sorumluluklarının olması beklenmektedir. Bunlara benzer olarak, kurumların yönetişim mekanizması kapsamında siber risklerden korunmaya yönelik olarak geliştirdikleri yönetim prensipleri, yerel ve küresel yasal çerçeve ile birlikte uluslararası standartlar da periyodik olarak gözetilerek, mevzuata uyumun kontrol edilmesi zorunludur (Pickett, 2011:211).

Veri türevi varlıkların gizlilik, bütünlük ve erişilebilirlik kriterlerinin temin edilmesi için alınan önlemler, yapılan planlamalar ve işletilen süreçler siber güvenlik faaliyetlerini oluşturmaktadır (Ryder & Madhavan, 2019). Siber güvenlik, entelektüel sermayeyi, teknoloji çevresini ve araçlarını kapsayan ve bir sistem geliştirme döngüsünde yer alan yasaların, standartların ve politikaların çerçevesinde yenilenen süreçlerden oluşmaktadır. Bu nedenle, siber güvenlik faaliyetlerinin bir yönetişim mekanizması dahilinde tasarlanması siber saldırıların önüne geçilmesinde anahtar rol oynamaktadır (Schreider, 2019:75). Ayrıca, siber güvenlik içindeki süreçlerin tolerans limitlerinin belirlenerek nominal bir savunma sisteminin tasarımı için risk takipleri yapılmalıdır. Risk yönetimi planlaması yapılırken, kurumun bulunduğu sektör, faaliyet alanları, iş yapış biçimleri, organizasyonel kültürü, teknolojik altyapısı ve konumlandığı bölgeler tanımlanarak, yasal mevzuata uyumluluk açısından uygun bir yönetişim çerçevesi kurgulanmalıdır (Calder, 2005:30). Bu doğrultuda, organizasyonların bilgi teknolojileri altyapılarını hem ulusal yasal çerçeve hem de uluslararası standartlar açısından biçimlendirmeleri gerekmektedir. Ancak, yönetişim, risk ve uyumluluk açısından siber güvenlik fonksiyonlarının dinamik olarak güncelleştirilmesi için kullanılan yöntemlerde kısmen tutarsızlıklar gözlemlenebilmektedir. Bunun nedeni ise teknolojinin hızlı değişimine yasal mevzuatın ve standartların adaptasyonunun geride kalmasıdır. Bu bağlamda, iç denetçilerin bilgi teknolojisi kontrollerinde üstlendikleri sorumluluklar, siber güvenlik yönetimi resminin, risk ve uyumluluk perspektifinden nasıl çizilmesi gerektiği üzerine önemli bulgular sunmaktadır.

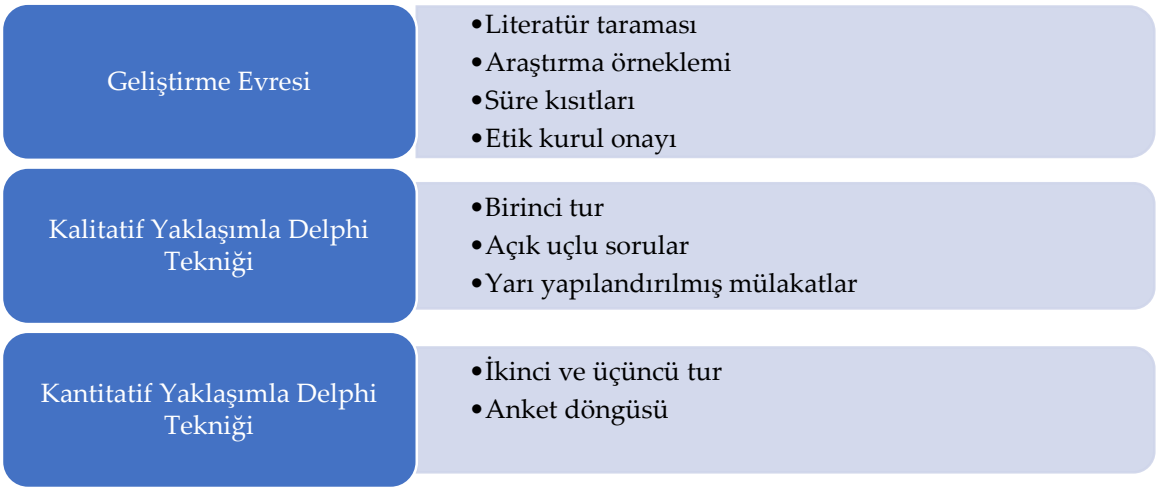
Siber güvenlik sistemlerinin etkin bir biçimde kontrol edilmesi için insan etmeninden kaynaklanan güvenlik açıklarının minimize edilmesi ve bu türden hataların önüne geçilmesi birincil önem arz etmektedir. Bu nedenle, kurumlarda organizasyonel kültürün ve farkındalığın zemininin kurulması ve iyileştirilmesi için etik davranış standartlarının oluşturulması ve uygulanması gereklidir (KPMG's Audit Committee Institute, 2017:18). Özellikle, siber güvenlik gibi hassaslık derecesi yüksek süreçleri içeren bir faaliyet alanı için, risklerin kontrol edilebilir limitler arasında tutulması, ancak ve ancak, kurum içi disiplinin ve yönetişimin verimli olarak sağlanması ile mümkün kılınabilir. Siber güvenlik yönetimi, organizasyonel davranışın, yönetsel süreçler ile sentezlenerek, teknik ve operasyonel kontrollerin yasalara ve standartlara uyumlu hale getirilmesi için gereken eylemlerin önceden planlanması ile iyileştirilebilir. Bu doğrultuda, kurumlarda siber güvenlik faaliyetlerinin işlerliğinin içsel açıdan hangi durumda olduğunun kontrol edilmesi için belli kriterlere ihtiyaç duyulmaktadır. Bu kriterlerde, etik kurallar kapsamına dahil edilerek, bilgi teknolojileri denetimi faaliyetlerinin, kurum içi kültüre yayılması sağlanabilir ve bu sayede etkin bir siber güvenlik yönetişimi kurulabilir. Bu yüzden, iç denetim açısından, siber güvenlik yönetişimi süreçlerinin sağlıklı olarak sürdürülebilmesi için, kurumun

faaliyetlerini yürüttüğü bölgenin yasaları, uluslararası standartlar ve kurumsal yönetim ilkelerinin uygulanış şeklini gösteren etik kuralların incelenmesi gereklidir.

Sonuç olarak, iç denetimin siber güvenlik yönetişimi kapsamındaki fonksiyonlarının, bilhassa banka sektörü gibi müşteri verilerinin birincil derecede kritik öneme sahip olduğu ve işletme süreçlerinin dijital olarak gerçekleştirildiği bir örneklem penceresinden incelenmesi, hem bankaların siber risk kontrol sistemlerinin hangi yasalara ve standartlara göre kurgulandığının aydınlatılması hem de iç denetiminin bilgi teknolojileri gözetimlerindeki aktivitelerinin incelenmesi açısından önem taşımaktadır. Tüm bu varsayımlar doğrultusunda, doktora tezi kapsamında gerçekleştirilen aktivitelerden türetilen bu çalışmada tez sorunsalına ilişkin olarak incelenen kuramsal çerçeve ve buna yönelik dizaynı yapılan araştırma metodolojisi sunulmuştur.

2. YÖNTEM

Çalışmanın sorunsalı, keşifsel sıralı karma yöntemler araştırma tasarımı doğrultusunda delphi tekniğinin uygulanması ile aydınlatılmaya çalışılacaktır. Belirlenen araştırma yöntemine göre, öncelikle, çalışmanın kalitatif kısmı kapsamında, açık uçlu sorulardan yarı yapılandırılmış görüşmeler ile görsel-işitsel ve yazılı olarak elde edilen metinsel veriler anlamlı hale getirilerek ikinci aşamada yer alacak nicel bölümün hazırlık aşaması tamamlanmış olacaktır. Genel olarak, bu tip bir araştırma yönteminde, kalitatif kısım elde edilen verilerin sınıflandırılmasında rol oynarken, kantitatif bölüm için araştırmacıya rehberlik eder (Creswell, 2014:200). Çalışmanın araştırma yöntemi, delphi tekniği üzerinden biçimselleştirilerek nitel verilerin yarı yapılandırılmış mülakat ve anket yollarıyla elde edilmesini, sınıflandırılmasını ve nicel olarak analiz edilmesi süreçlerini kapsamaktadır.



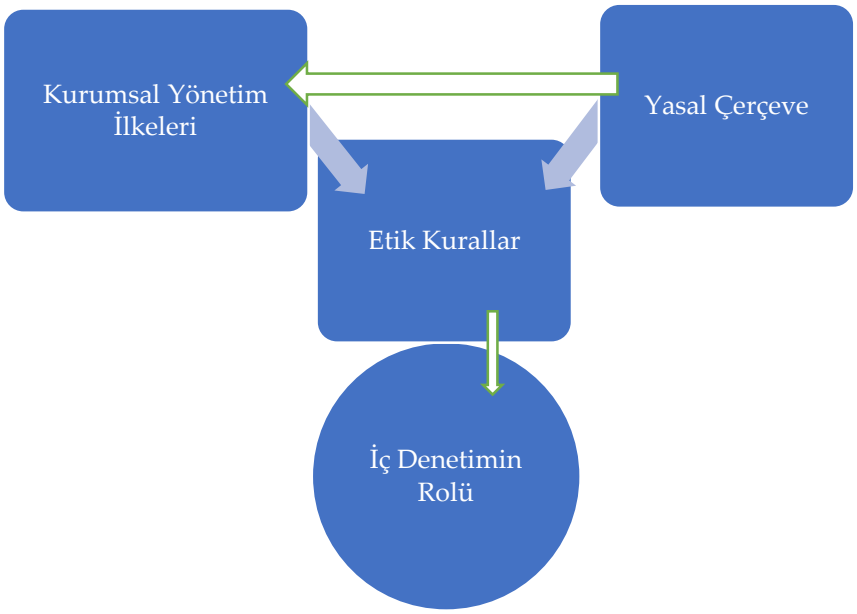
Şekil 1. Araştırma Tasarımı

Öncelikle, taslak olarak oluşturulan şemaya göre, araştırmanın planı bir sistematiğe yerleştirilerek sırasıyla süreçlerin işlenmesi gerçekleştirilmiştir. Tez araştırmasının içeriğinde tanımlanan bu yol haritası dahilinde öncelikle geniş çaplı bir literatür incelemesi yapılmıştır. Bu çalışma makale niteliği taşıması ve tezin araştırma kısmına ilişkin bölümlerden kesitler sunması hasebiyle, geçmiş çalışmaların kümelemesi tezin araştırma yöntemine ilişkin bilimsel makaleler bazında yapılmıştır.

Konuya ilişkin olarak öne sürülen teorik önermelerden ve gerçekleştirilen uygulamalı araştırma çalışmalarından elde edilen bulgulara göre yönetişim, siber risk kontrolü ve yasal çevreye uyumluluk mekanizması kapsamındaki parametrelerin araştırma sorunsalına yönelik olarak incelenebileceği çıkarımında bulunulmuştur. Bu nedenle, tez çalışmasının kavramsal kısmında yönetişim, risk ve uyumluluk değişkenleri derinlemesine bir biçimde mercek altına alınarak,

araştırmanın uygulama kısmına yönelik olarak süzgeçten geçirilmiştir. Bu bağlamda, iç denetimin siber güvenlik yönetişimi ile bağının oluşmasında ön plana çıkan değişkenler etik kurallar, kurumsal yönetim ilkeleri ve yasal çerçeve olarak belirlenmiştir.

Bankalardaki siber güvenlik yönetişiminin sağlanmasında insan odaklı risklerin kontrol altına alınması amacının birincil önceliğe sahip olabileceği varsayımından yola çıkılarak, bağımsız değişken olarak belirlenen yasal çerçevenin, etik kuralların oluşumunda ve icra edilmesinde hem doğrudan hem de kurumsal yönetim ilkeleri üzerinden dolaylı olarak etkili olabileceği ihtimali üzerinde durulmuştur.



Şekil 2. Araştırma Değişkenlerinin İlişkisel Gösterimi

Bu çalışmada, amaçlı örnekleme, araştırmacıya takip edeceği nitel araştırma yönteminin çeşidinden bağımsız olarak geliştireceği çalışmanın içeriği doğrultusunda profesyonel olarak tecrübeli ve bilgili kişileri niyetli bir yaklaşımla seçme olanağı tanıyan bir metot olması nedeniyle kullanılmıştır. Patton'un da belirttiği gibi nitel bir araştırmanın geçerliliği örneklem hacminden ziyade katılımcı profilinin araştırma konusuna hangi düzeyde hâkim olduğu ile ölçülebilir (Conway, 2020:18).

Bahsedilen nedenlerden ötürü, amaçlı örnekleme yöntemi ile ana kütleden, yani bu araştırma için banka sektörü olarak tanımlanan örnek uzaydan, iradi olarak seçilen bankalarda rol alan yöneticilerin, takım liderlerinin, uzmanların, yasa düzenleyici kurumlardaki ilgili kişilerin ve konuya ilişkin araştırmaları olan akademisyenlerin görüşlerine ulaşılmak hedeflenmiştir. Şekil üçte gösterildiği üzere, Türkiye'deki banka sektörünü hedef alan ana kütle içerisinden kamu, özel, yabancı sermayeli, mevduat ve katılım olmak üzere kısımlara ayrılan kurumlardan örnekleme yapılmıştır. Özellikle, siber risklerin daha yüksek olasılıkla karşılaşıldığı, internet bankacılığının sıklık oranının yüksek olduğu bankalar örnekleme dahil edilmeye çalışılmıştır. Örneklem hacmi nicel olarak on beş katılımcı ile sınırlandırılarak araştırma sorunsalına yönelik geri beslemelere ulaşılmak amaçlanmıştır.

Araştırmaya iştirak eden katılımcıların;

- Konuyla ilgili yetkinliklerinin en azından uzmanlık seviyesinde olduğu;
- Açık uçlu sorulara ve anket ifadelerine objektif ve bağımsız olarak cevap verdikleri;

- Sundukları bilgilerin araştırmanın kontrol değişkenlerine yönelik olarak genel algıyı ifade edebilecek düzeyde olduğu;

varsayılmıştır.

Araştırma çalışması;

- Delphi araştırmasına katılan panelistlerin kişisel düşünceleri ve ifadeleri;
- Nitel ve nicel veri analizleri;
- Etik kurallar, kurumsal yönetim ilkeleri ve yasal çerçeve olarak belirlenen değişkenler;
- Siber güvenlik ve denetim alanında faaliyet gösteren kişilerin katılımı;
- Siber güvenlik, iç denetim ve etik kurallar üzerine çalışmaları olan akademisyenlerin katılımı;
- Yasa düzenleyici kurumlarda bilgi sistemleri, siber güvenlik ve banka sektörü üzerine rol alan kişilerin katılımı;
- 1 Mart 2021 ile 31 Aralık 2021 arası olarak belirlenen veri toplama süresi;

ile sınırlandırılmıştır.

Çalışmanın sorunsalı, keşifsel sıralı karma yöntemler araştırma tasarımı doğrultusunda delphi tekniğinin uygulanması ile aydınlatılmaya çalışılacaktır. Belirlenen araştırma yöntemine göre, öncelikle, çalışmanın kalitatif kısmı kapsamında, açık uçlu sorulardan yarı yapılandırılmış görüşmeler ile görsel-işitsel ve yazılı olarak elde edilen metinsel veriler anlamlı hale getirilerek ikinci aşamada yer alacak nicel bölümün hazırlık aşaması tamamlanmış olacaktır. Genel olarak, bu tip bir araştırma yönteminde, kalitatif kısım elde edilen verilerin sınıflandırılmasında rol oynarken, kantitatif bölüm için araştırmacıya rehberlik eder (Creswell, 2014:59).

Bahsedilen nedenler ışığında, delphi tekniği karma yöntem araştırması kapsamında kullanılarak, öncelikle açık uçlu sorular vasıtasıyla veriler elde edilmeye çalışılmıştır.

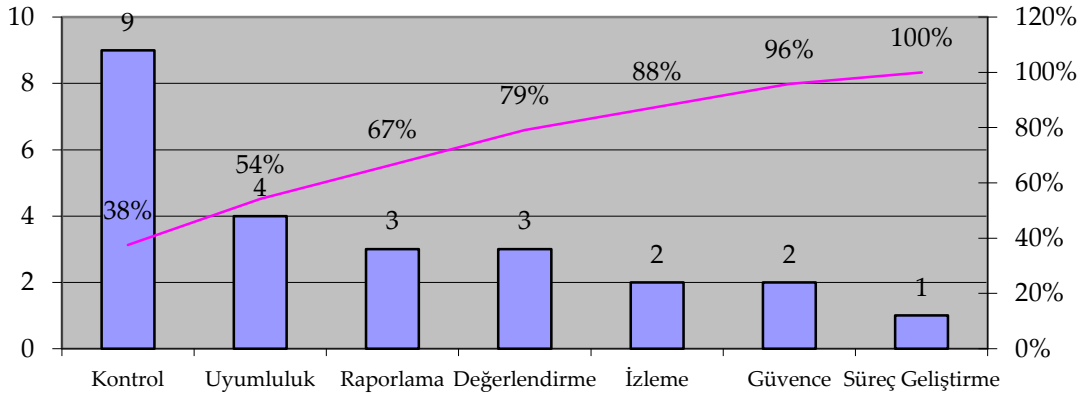
Katılımcılara, delphi yönteminin ilk turu çerçevesinde yöneltilen açık uçlu sorular sırasıyla belirtilmiştir;

- İşletmenizde, siber güvenlik hizmetleri dahilinde, iç denetçiler hangi süreçlerde sorumluluk üstlenmektedir?
- Kurumunuzda, iç denetimin, siber güvenlik kapsamında yürütülen fonksiyonlarının yeterlilik düzeyini nasıl ifade edersiniz?
- Siber güvenlik ile ilgili sorunlarda, iç denetim ve yönetim kurulu arasındaki etkileşim mekanizması nasıl oluşturulmaktadır?
- Organizasyonunuz değerlendirmeye alındığında, gizlilik, bütünlük ve kullanılabilirlik kavramları sizde nasıl bir çağrışım yapmaktadır?
- Etik kurallar, iç denetim ve siber güvenlik kavramları ile birlikte değerlendirildiğinde, sizde neleri çağrıştırmaktadır?
- Size göre, organizasyonunuzda, etik kurallar, iç denetimin siber güvenlik süreçlerinde üstlendiği rolü gerçekleştirirken takip ettiği yöntemler açısından nasıl tanımlanmaktadır?
- Kurumunuzda, siber güvenlik yönetiminde yer alan yasal çerçevenin ve uluslararası standartların gözetilmesi süreçlerinde iç denetim nasıl bir rol üstlenmektedir?

Katılımcılara yöneltilen sorular çerçevesinde toplanan metinsel veriler, Nvivo 12 programı vasıtasıyla ayıklanarak, pareto grafikleri ve balık kılçığı diyagramı ile kök neden analizleri yapılarak sınıflandırılmıştır.

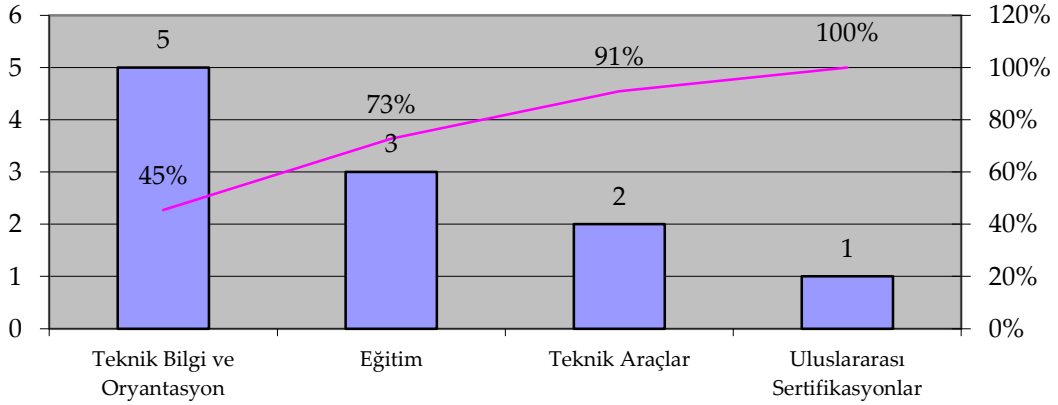
3. BULGULAR

Katılımcıların ilk soruya ilettikleri kişisel cevapları doğrultusunda elde edilen ham verilerin işlenmesi sonucunda, iç denetçilerin siber güvenlik kapsamında, ağırlıklı olarak, risk yönetimi faaliyetlerinin yasal çerçeveye uyumlulukları dahilindeki kontrolleri, değerlendirilmeleri ve raporlanmaları ön sıralarda yer almıştır. İç kontrol birimlerinin sorumluluğunda sürdürülen risk yönetimi işlemlerinin geçerli olduklarına dair güvence sunarak bu süreçlerin gelişimine katkıda bulunma da iç denetçilerin fonksiyonları arasında belirtilmiştir.



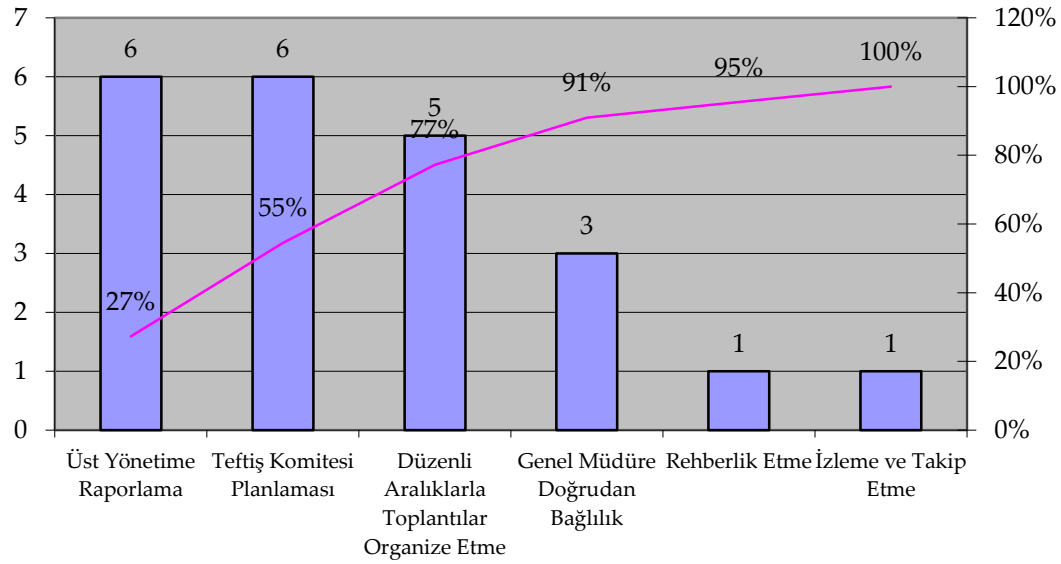
Şekil 3. Pareto Grafiği 1

İç denetçilerin siber güvenlik yönetimindeki etkinliklerinin yeterlilik derecesi genel olarak kabul edilebilir seviyelerde olarak belirtilirken, bu seviyenin yukarıya çıkarılması için denetim ekiplerinin siber güvenlik ile ilgili dijital platformları, yazılımları, araçları ve donanımları daha etkin kullanabilmesi için kurum içi eğitimlerin ve oryantasyon programlarının düzenlenmesi gerektiği üzerinde duruldu. Denetçilerin, bilgi teknolojileri kapsamındaki faaliyetlerini en üst seviyelerde gerçekleştirmeleri için uluslararası sertifikasyon programlarına katılabilecekleri ve bu sayede kendi yetkinliklerini bilerek ve belgeleyerek siber güvenlik kontrollerini sürdürebilecekleri bildirildi. Bunlara paralel olarak, kontrolörlerin, Sertifikalı Bilgi Sistemi Denetçisi (Certified Information System Auditor) (CISA) ve Sertifikalı Etik Bilgisayar Korsanı (Certified of Ethical Hacker) (CEH) olarak bilgi teknolojileri denetimlerinde rol almalarının siber güvenlik yönetişimindeki süreçlerde etkinliği geliştirebileceği üzerinde duruldu.



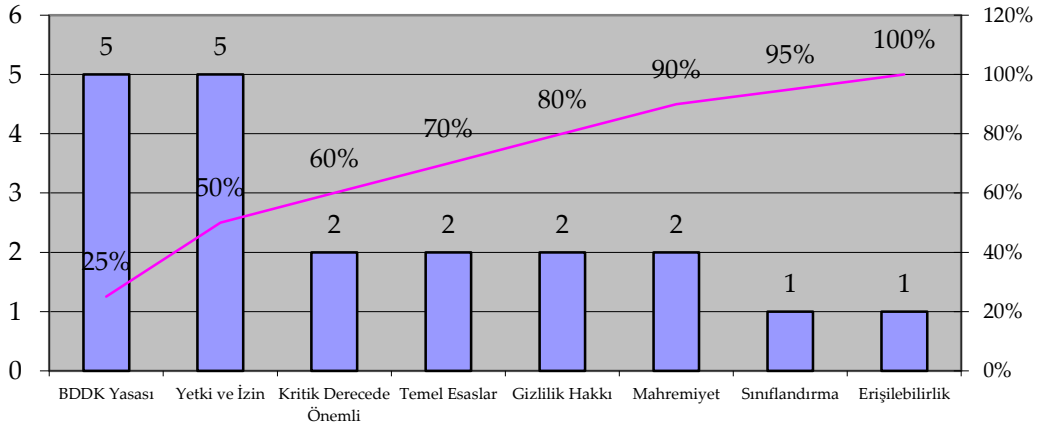
Şekil 4. Pareto Grafiği 2

İç denetçilerin siber güvenlik süreçlerinde kurum içi yönetişim kapsamındaki rolü iç kontrol faaliyetlerinin üst yönetime raporlanmasını, teftiş komitesi toplantılarının düzenlenerek periyodik aralıklarla toplantıların organize edilmesini ve süreç geliştirme konularında izleme, takip etme ve rehberlik yapılmasını kapsamaktadır. Bu çalışmalar sürdürülürken, süreçler ile ilgili genel müdürü doğrudan bilgilendirme prensibi esas alınmaktadır.



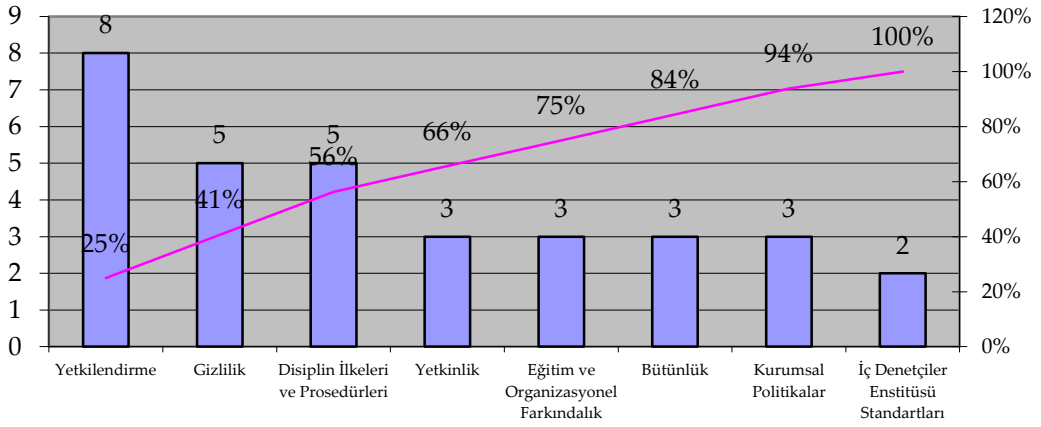
Şekil 5. Pareto Grafiği 3

Gizlilik, bütünlük ve kullanılabilirlik veya diğer bir deyişle enformasyonun kullanıma hazır tutulması perspektifinden farkındalık ölçülmesine yönelik olarak katılımcılara iletilen sorudan elde edilen verilerin göstergesinde Bankacılık Düzenleme ve Denetleme Kurumu (BDDK) yasasının, kritik verilere erişilebilirliğin yetki ve izin hiyerarşisi sınırları dahilinde kullanılabilmesinde yol gösterici olduğu izlenimine varılmıştır. Ayrıca, katılımcılar bu kavramların, siber güvenlik süreçlerinin sağlıklı sürdürülmesinde temel esaslar olarak algılanması gerektiği üzerinde durarak, kritik öneme sahip olduklarını bilhassa vurgulamışlardır.



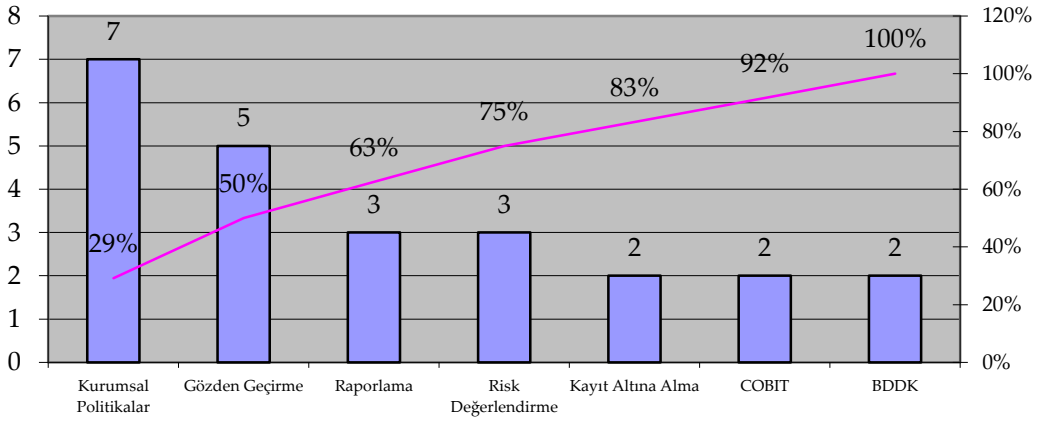
Şekil 6. Pareto Grafiği 4

Katılımcılar, etik kuralların siber güvenlik süreçlerinde de diğer iş akışlarındaki hassasiyete paralel olarak organizasyonel kültüre entegre olmaları gerektiği üzerinde durarak, siber risklerden korunmak için birer disiplin ilkesi ve prosedür olarak algılanıp kurumsal politikalar ile senkronize yaklaşımlarla oluşturulmaları gerektiklerini vurgulamışlardır.



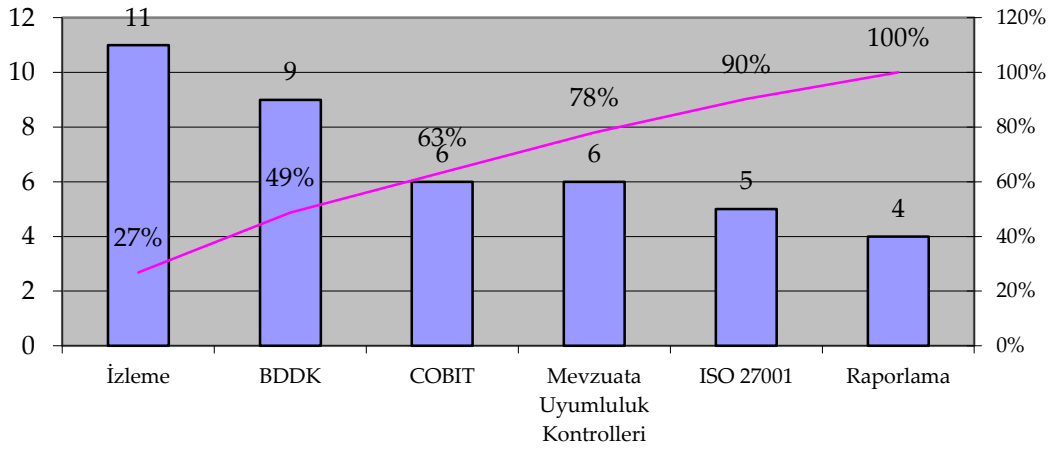
Şekil 7. Pareto Grafiği 5

İç denetimin siber güvenlik süreçlerindeki fonksiyonları dahilinde etik kuralların nasıl algılandığına dair katılımcılara yöneltilen soruya ise yüksek oranda kurumsal politikalar yanıtı alınmıştır. Etik kurallara uyumluluğun hangi kriterlere göre tanımlandığı ve ölçüldüğü ise Bilgi ve İlgili Teknolojiler için Kontrol Hedefleri (Control Objectives for Information and Related Technology) (COBIT) kriterleri ve BDDK yasaları ile çerçevelenmiştir. Etik kurallara uyumun kontrolünde ise gözden geçirme, raporlama, risk değerlendirme ve kayıt tutma ağırlıklı olarak vurgulanan süreçler olmuşlardır.



Şekil 8. Pareto Grafiği 6

İç denetimin siber güvenlik yönetişimi faaliyetlerinin yürütülmesinde üstlendiği rolün yasalara ve uluslararası standartlara, yani mevzuata uyumluluk perspektifinden nasıl sağlandığına dair katılımcılara yöneltilen soruya, ağırlıklı oranda BDDK'nın önderliğinde cevabı alınmıştır. Benzer olarak, iç denetimin siber güvenlik yönetimindeki rolünü gerçekleştirmesinde COBIT ve Uluslararası Standartlar Örgütü (International Organization for Standardization) ISO 27001 esasları referans düzlemi olarak belirtilmiştir. Bu bağlamda, izleme, mevzuata uyumluluğun kontrol edilmesi ve raporlama faaliyetleri yoğunluklu olarak katılımcıların bahsettiği süreçler olmuşlardır.



Şekil 9. Pareto Grafiği 7

Pareto grafikleri ve balık kılçığı diyagramı ile tasnifi yapılan işlenmiş veriler doğrultusunda, delphi tekniğinin ikinci turu için tasarlanacak anketin hazırlık aşamasına geçilmiştir. Anket beşli likert ölçeğine uygun biçimde, birinci turda yapılan sınıflandırma baz alınarak hazırlanmıştır.

Delphi yönteminin ikinci kısmı doğrultusunda, tüm katılımcılara çevrimiçi olarak iletilen anket çalışmasına tüm katılımcılar yanıtlarını sunmuşlardır. Bu kısımda, öncelikli olarak, anket vasıtasıyla elde edilen kategorik değişken sınıfında yer alan sıralı veriler merkezi yayılım ölçüleri doğrultusunda istatistiksel olarak anlamlı bilgilere dönüştürülmek için nicel analize tabi tutulmuşlardır. Bu bağlamda, ankette yer alan her ifade için çeyrekler açıklığı metriğinin bir veya birden küçük bir değer olup olmadığı ve en azından yüzde yetmiş beş oranında fikir birliğine varılıp varılmadığı kontrol edilmiştir.

Sorumluluk değişkeni baz alınarak hazırlanan anket ifadelerinin tümünde fikir birliğine varılmıştır ve delphi yönteminin uygulanma biçimi gereği, bu parametre için üçüncü bir anket döngüsüne ihtiyaç kalmamıştır.

Tablo 1. Sorumluluk Kapsamındaki İfadelerden Elde Edilen Verilerin Analizleri

Sorumluluk	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, siber güvenlik kapsamında elde edilen bulguların kapanmasından sonra, gerekli kontrollerin yapılmasında rol alır.	4,466667	0,498887652	4	1	15 (100%)	0 (0%)	0 (0%)	Sağlanmıştır
İç denetim, BDDK'nın 15 Mart 2020'de yayınlamış olduğu yönetmelik çerçevesinde siber güvenliğe ilişkin yıllık kontrollerde bulunmaktadır.	4,333333	0,699205899	4	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim, bağımsız denetim firmalarının gerçekleştirmiş oldukları sızma testi bulgularının kapatıldıktan sonra teyit edilmesi fonksiyonuna sahiptir.	4,466667	0,718021974	5	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim, siber güvenlik kapsamındaki güvenlik açıklarının tespit edilmesinde fonksiyona sahiptir.	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim, siber güvenlik ile ilgili bulguların genel müdüre veya yönetim kuruluna doğrudan raporlanmasında sorumluluk sahibidir.	4,533333	0,618241233	5	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır

İç denetim ekiplerinin siber güvenlik yönetimi süreçlerinde ihtiyaç duyabilecekleri yetkinlikleri belirlemek ve değerlendirmek için hazırlanan ifadelerden altıncısı hariç, yedinci, sekizinci dokuzuncu ve onuncu ifadelerde fikir birliği sağlanamamıştır. Bu nedenle, bu ifadeler için, cevapları ortalamadan sapmaya neden olan katılımcılar için üçüncü turun yapılmasına karar verilmiştir.

Tablo 2. Yetkinlik Kapsamındaki İfadelerden Elde Edilen Verilerin Analizleri

Yetkinlik	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, BDDK'nın tasarladığı yönetmelikler kapsamında bilgi güvenliğine yönelik hazırlanan kontrol listelerinin denetlenmesi sürecini bilgi teknolojisi denetçilerinden destek alarak yürütmelidir.	4,6	0,489897949	5	1	15 (100%)	0 (0%)	0 (0%)	Sağlanmıştır
İç denetim, BDDK'nın bilgi sistemleri yönetmeliği doğrultusunda icra etmekte olduğu denetim faaliyetlerini sürdürmek için temel seviyede yazılım bilgisine sahip olmalıdır.	4,066667	0,77172246	4	2	11 (73%)	4 (27%)	0 (0%)	Sağlanamamıştır
İç denetim, bağımsız denetim firmalarının gerçekleştirmiş oldukları sızma testi bulgularının kapatıldıktan sonra kontrol edilmesi ve onaylanması süreçlerinde etkin olmak için sistem ve ağ yönetimi bilgisine sahip olmalıdır.	4	0,894427191	4	2	11 (73%)	3 (20%)	1 (7%)	Sağlanamamıştır
İç denetim, BDDK'nın tasarladığı yönetmelikler kapsamında bilgi güvenliğine	3,933333	0,679869268	4	1	11 (73%)	4 (27%)	0 (0%)	Sağlanamamıştır

yönelik hazırlanan kontrol listelerinin denetlenmesi sürecinde etkin olmak için bilgi güvenliği mimarisi ve altyapısı üzerine teknik düzeyde bilgiye ve yeterli tecrübeye sahibi olmalıdır.								
İç denetim, siber güvenlik kapsamında sürdürdüğü gözetim faaliyetlerinde etkin rol almak için SIEM araçlarını kullanmaya hâkim olmalıdır.	3,8	0,909212113	4	1	11 (73.3%)	2 (13.3%)	2 (13.3%)	Sağlanamamıştır

Ankette, yönetişim bazında hazırlanan ifadelerin katılımcılara iletilmesi ile elde edilen verilerin sonucunda, on bir, on üç ve on beş sıra numaralı öne sürümlerde fikir birliğinin sağlanamadığı ortaya çıkmıştır. İleri sürülen bu ifadelerin, delphi yönteminin üçüncü turu kapsamında, ortalamadan anlamlı olarak sapmaya neden oldukları için katılımcılara tekrar sorulmalarına karar verilmiştir.

Tablo 3. Yönetişim Kapsamındaki İfadelerden Elde Edilen Verilerin Analizleri

Yönetişim	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, yönetim kurulu, genel müdür ve bilgi teknolojileri departmanı arasındaki yönetişimde danışmanlık rolüne sahiptir.	3,666667	0,788810638	4	1	9 (60%)	5 (33.3%)	1 (6.7%)	Sağlanamamıştır
Siber güvenlik kapsamında faaliyetlerini sürdüren iç denetçilere gerekli eğitimler	4,666667	0,471404521	5	1	15 (100%)	0 (0%)	0 (0%)	Sağlanmıştır

organize edilmelidir.								
İç denetim, siber güvenlik denetimlerinde doğrudan yetkiye sahip olmalıdır.	3,733333	0,928559218	4	1	10 (66.6%)	3 (20%)	2 (13.3%)	Sağlanamamıştır
İç denetim, siber güvenlik denetimlerinde danışmanlık rolü ile destekleyici konumundadır.	3,8	0,8326664	4	0	12 (80%)	1 (6.7%)	2 (13.3%)	Sağlanmıştır
İç denetim, siber güvenlik ile ilgili vakalarda gerekli bilgilendirmeyi düzenli aralıklar ile üst yönetime yapmakta sorumluluğa sahiptir.	3,8	0,909212113	4	1	11 (73%)	2 (13.3%)	2 (13.3%)	Sağlanamamıştır

Anketin dördüncü kısmı kapsamında yer alan ve iç denetimin siber güvenlik yönetimi süreçlerindeki faaliyetlerinde gizlilik, bütünlük ve erişilebilirlik kavramlarının hangi ölçüde ve nasıl gözetildiğine dair katılımcılara yöneltilen yargılardan tümünde fikir birliğine varılması nedeniyle, bu bölüm için üçüncü bir raunda gerek kalmamıştır.

Tablo 4. Gizlilik, Bütünlük ve Erişilebilirlik Dahilindeki İfadelerden Elde Edilen Verilerin Analizleri

Gizlilik, Bütünlük ve Erişilebilirlik	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, siber güvenlik kapsamındaki süreçlerde rol alırken denetim kanıtlarını gizlilik, bütünlük ve erişilebilirlik prensiplerine uygun olarak kayıtlara almalı, muhafaza etmeli ve raporlamalıdır.	4,4	0,711805217	5	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır

İç denetim, siber güvenlik kapsamındaki faaliyetlerini yetki prensibine göre yürütmelidir.	4,333333	0,699205899	4	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim, siber güvenlik kapsamında gerçekleştirdiği faaliyetler sonucu elde ettiği bulguların erişiminin aksamadan gerçekleşmesini sağlamalıdır.	4,066667	0,573488351	4	0	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim, siber güvenlik kapsamında sürdürdüğü aktivitelerin sonucunda elde ettiği bulguların herhangi bir şekilde değiştirilmediğine dair güvence sağlamalıdır.	4,2	0,54160256	4	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır
İç denetim, siber güvenlik kontrollerinde elde edilen bulguların yetkisi olmayan kişilere iletilmiyor olduğuna dair güvence sağlamalıdır.	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır

Anketin beşinci kısmında, kurumsal yönetim ilkelerinin iç denetimin siber güvenlik yönetişimi içindeki fonksiyonlarına etkisini ölçmek için katılımcılara yöneltilen önermelerin tümünden fikir birliğine varıldığı çıkarımı yapılmıştır. Bu bağlamda, üçüncü bir tura gerek kalmamıştır.

Tablo 5. Kurumsal Yönetim İlkeleri Kapsamındaki İfadelerden Elde Edilen Verilerin Analizleri

Kurumsal Yönetim Prensipleri	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, siber güvenlik kapsamındaki fonksiyonlarını gerçekleştirirken yasal çevreyi takip ederek, gerekli bilgilendirmeleri yapmalıdır.	4,2	0,54160256	4	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır

İç denetim, siber güvenlik kapsamındaki faaliyetlerini sürdürürken yasa dışı herhangi bir sürece dahil olmadan meslek ahlakına uygun biçimde aktivitelerde bulunmalıdır.	4,6	0,611010093	5	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır
İç denetim, siber güvenlik kapsamındaki faaliyetlerini gerçekleştirirken kurumun etik prensiplerine ve yönetim ilkelerine saygılı bir biçimde işlemlerini yürütmelidir.	4,533333	0,618241233	5	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır
İç denetim ekipleri, siber güvenlik dahilindeki süreçlerde rol alırlarken bilgilerine, yetkinliklerine ve tecrübelerine uygun görevleri üstlenmelidirler.	4,333333	0,596284794	4	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır
İç denetim ekipleri, siber güvenlik dahilindeki süreçlerde rol alırlarken kabiliyetlerini, etkinliklerini ve ürettikleri hizmetin kalite seviyesini gelişme sürecindeki teknolojiler doğrultusunda sürekli iyileştirmelidirler.	4,4	0,611010093	4	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır

Bankalarda, etik kuralların siber güvenlik süreçlerine yeterince entegre olup olmadığını ve bu süreçlerdeki iç denetim faaliyetlerinin bu kurallara uygun olarak yürütülüp yürütülmediğini anlamaya yönelik olarak hazırlanan bu kısımdan elde edilen geri beslemeler doğrultusunda, otuzuncu yargıya yönelik fikir birliğine varılamamıştır. Bu nedenle, bu önerme için ilave bir tur daha yapılmasına karar verilmiştir.

Tablo 6. Etik Kurallar Kapsamındaki İfadelerden Elde Edilen Verilerin Analizleri

Etik Kurallar	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
Kurumlarda, etik kuralların kesin ve net olarak tanımlandığı ve belirtildiği yazılı dokümanlar olmalıdır.	4,333333	0,596284794	4	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır
Etik kuralların işlerliğinin denetlenmesinde etkin olarak işleyen bir raporlama mekanizması mevcut olmalıdır.	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
Etik kuralların, ihlal edilmesi durumunda raporlamanın doğrudan genel müdüre veya yönetim kuruluna yapılması gereklidir.	4,133333	0,618241233	4	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim ve siber güvenlik ekipleri etik kuralların ihlal edilmesine ilişkin durumlarda koordineli bir yaklaşımla bulgular elde etmelidirler.	4,066667	0,442216639	4	0	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır
İç denetim ekipleri kurumların mevzuata uyumluluğunu kontrol ederlerken, yasaların neden yenilendiğini de araştırmalıdırlar.	3,733333	1,06249183	4	2	10 (66.6%)	2 (13.3%)	3 (20%)	Sağlanamamıştır

Bankaların siber güvenlik yönetimi kapsamında sürdürdükleri süreçlerin uluslararası standartlara ve yerel çevredeki mevzuata uyumluluklarının kontrolünde iç denetim faaliyetlerinin hangi oranda ve nasıl kullanıldığını ölçmek için tasarlanan anketin yedinci kısmındaki yargıların tümünde görüş birliği sağlanmıştır.

Tablo 7. Yasal ve Uluslararası Politika Çerçevesi Kapsamındaki İfadelerden Elde Edilen Verilerin Analizleri

Yasal ve Uluslararası Politika Çerçevesi	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, BDDK'nın oluşturduğu yönetmelik ve uluslararası standartlar kapsamında oluşturulan kontrol listelerinin uyumluluğunu takip etmektedir.	4,333333	0,471404521	4	1	15 (100%)	0 (0%)	0 (0%)	Sağlanmıştır
Türkiye'deki bankacılık sektöründe bilgi güvenliği bağlamında mevzuata uyum çerçevesinde BDDK yönetmeliği, ISO 27001 ve COBIT 4.1 DS5 süreci dikkate alınmaktadır.	4,266667	0,77172246	4	1	14 (93%)	0 (0%)	1 (7%)	Sağlanmıştır
İç denetim, mevzuata uyum çerçevesindeki, gözetim faaliyetlerini sürdürürken tanımladığı kontrol eksikliklerini üst yönetime raporlamaktadır.	4,4	0,611010093	4	1	14 (93%)	1 (7%)	0 (0%)	Sağlanmıştır
İç denetim ekipleri mevzuata uyumluluğa ilişkin sürdürdükleri faaliyetlerde süreç teftişlerinde bulunmaktadırlar.	4,066667	0,679869268	4	1	12 (80%)	3 (20%)	0 (0%)	Sağlanmıştır
Türkiye'de faaliyet gösteren tüm bankalar BDDK'nın 5411 sayılı bankacılık kanununa göre bilgi sistemlerini yapılandırmaktadırlar.	4,133333	1,024152766	4	1	13 (87%)	1 (7%)	1 (7%)	Sağlanmıştır

Delphi tekniğinin yol haritası doğrultusunda gerçekleştirilen ikinci raunt kapsamındaki anket vasıtasıyla elde edilen verilerin analizleri istikametinde sağlanan çıkarımlar ile fikir birliğine varılamayan görüşler için üçüncü bir tur daha organize edilmiştir. Bu bölümün amacı, fikir birliğine varılamayan yargıların, çoğunluğun fikrinden anlamlı bir sapma gösteren cevapları olan

katılımcılara tekrar yönlendirilmesi ile yeniden elde edilen verilerden ulaşılacak çıkarımların sonuca nasıl tesir ettiğini göstermektir.

İkinci turda yetkinlik kriteri bazında görüş birliğinin sağlanamadığı ifadelerin üçüncü tur kapsamında yeniden katılımcılara sunulmasıyla elde edilen verilerin analizi sonucunda yetkinlik kümesindeki tüm yargılarda fikir birliği sağlanmıştır.

Tablo 8. Yetkinlik

Yetkinlik	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, BDDK'nın bilgi sistemleri yönetmeliği doğrultusunda icra etmekte olduğu denetim faaliyetlerini sürdürmek için temel seviyede yazılım bilgisine sahip olmalıdır.	4,2	0,653197265	4	1	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim, bağımsız denetim firmalarının gerçekleştirmiş oldukları sızma testi bulgularının kapatıldıktan sonra kontrol edilmesi ve onaylanması süreçlerinde etkin olmak için sistem ve ağ yönetimi bilgisine sahip olmalıdır.	4,066667	0,853749898	4	1	12 (80%)	2 (13.3%)	1 (6.7%)	Sağlanmıştır
İç denetim, BDDK'nın tasarladığı yönetmelikler kapsamında bilgi güvenliğine yönelik hazırlanan kontrol listelerinin denetlenmesi sürecinde etkin olmak için bilgi güvenliği mimarisi ve altyapısı üzerine teknik düzeyde bilgiye ve yeterli tecrübeye sahibi olmalıdır.	4,066667	0,573488351	4	0	13 (87%)	2 (13%)	0 (0%)	Sağlanmıştır
İç denetim, siber güvenlik kapsamında sürdürdüğü gözetim faaliyetlerinde etkin rol almak için SIEM araçlarını kullanmaya hâkim olmalıdır.	4	0,730296743	4	0	13 (86.6%)	1 (6.7%)	1 (6.7%)	Sağlanmıştır

Yönetişim kriterleri bazında üçüncü turda katılımcılara yeniden yöneltilen görüşlerden on üçüncüsünde yeterli çoğunluk yine sağlanamamıştır. On birinci ve on beşinci ifadeler için ise fikir birliği sağlanmıştır.

Tablo 9. Yönetişim

Yönetişim	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim, yönetim kurulu, genel müdür ve bilgi teknolojileri departmanı arasındaki yönetişimde danışmanlık rolüne sahiptir.	3,866667	0,718021974	4	0	12 (80%)	2 (13.3%)	1 (6.7%)	Sağlanmıştır
İç denetim, siber güvenlik denetimlerinde doğrudan yetkiye sahip olmalıdır.	3,733333	0,928559218	4	1	10 (66.6%)	3 (20%)	2 (13.3%)	Sağlanmamıştır
İç denetim, siber güvenlik ile ilgili vakalarda gerekli bilgilendirmeyi düzenli aralıklar ile üst yönetime yapmakta sorumluluğa sahiptir.	4,066667	0,679869268	4	0	14 (93%)	0 (0%)	1 (7%)	Sağlanmıştır

Etik kurallara yönelik olarak görüşlerinde çoğunluğun fikir birliğinden sapma olan katılımcılara, yeniden sunulan otuzuncu soru için ise üçüncü turda uzlaşma sağlanmıştır.

Tablo 10. Etik Kurallar

Etik Kurallar	Ortalama	Standart Sapma	Ortanca	Çeyrekler Açıklığı	Sıklık			Fikir Birliği
					(4-5)	(3)	(1-2)	
İç denetim ekipleri kurumların mevzuata uyumluluğunu kontrol ederlerken, yasaların neden yenilendiğini de araştırmalıdırlar.	3,933333	0,928559218	4	1	12 (80%)	1 (7%)	2 (13%)	Sağlanmıştır

4. TARTIŞMA, SONUÇ VE ÖNERİLER

Yapılan bilimsel makaleler, delphi yönteminin sosyal bilimlerde gerçekleştirilen araştırma uygulamalarında nitel verilerin toplanmasında ve geleceğe yönelik önerilerin sunulmasında kullanıldığını ispat ederken, özellikle araştırma sorunsalına yönelik olarak çerçevelenen örneklemden seçilen uzmanların konuya ilişkin görüşleri arasındaki tutarlılığın istatistiksel olarak analiz edilmesi sonucunda oluşan fikir birliğinin değerlendirilmesi süreci ön plana çıkmaktadır.

Tablo 11. Delphi Yönteminin Kullanımına Yönelik Yazın İncelemesi

Yazar ve Yıl	Makale İsmi	Konu ve Kapsamı	Bulgular
Norman Crolee Dalkey(1967)	Delphi	Delphi metodolojisi ana hatlarıyla belirlenmiş sınırlar dahilinde açıklanmıştır.	Delphi yöntemi bir araştırma problemine yönelik olarak belirli bir kategori dahilindeki danışmanların veya uzmanların görüşlerinin istatistiksel analiz araçları ile süzgeçten geçirilerek uzun döneme hitap eden tahminler ve geleceğe yönelik fikirler sunmak için öne sürülmüştür.
Olaf Helmer-Hirchberg(1967)	Geleceğin Analizi, Delphi Yöntemi (Analysis of the Future, The Delphi Method)	Delphi metodu temel prensipleri ile açıklanmıştır.	Delphi tekniği sezgisel hükümlerin işletilmesi sonucu uzun dönem tahminlerin yapılması süreçlerini kapsar.
Gülsün Kurubacak (2007)	Açık ve Uzaktan Eğitimde Mobil Öğrenme için Araştırma Önceliklerinin ve İhtiyaçlarının Tespit Edilmesi: Bir Delphi Çalışması (Identify Research Priorities and Needs for Mobile Learning Technologies in Open and Distance Education: A Delphi Study)	Delphi tekniği açık ve uzaktan eğitimdeki mobil öğrenme teknolojileri kapsamındaki araştırma fırsatlarının tanımlanması ve kategorize edilmesi için uygulanmıştır.	Kısaca, internet üzerinden topluluğun yönetilmesi, kamu sorumluluğu ve dijital dönüşüme iştirak eden uzmanlar başlıca araştırma alanları olarak belirlenmiştir.

Gülsün Kurubacak (2011)	Çoğunluk için Uzaktan Öğrenme: Bilgi Toplumu Oluşturma Sürecinde Uzaktan Öğrenme Kültürü (E-learning for Pluralism: The Culture of E-learning in Building a Knowledge Society)	Uzaktan öğrenme için ihtiyaçlar ve itici güçler tanımlanarak tasnif edilmiştir.	Delphi yöntemi konuya ilişkin sorunları ve eleştirileri değerlendiren yirmi sekiz uzaktan öğrenme uzmanından, verilerin üç turda elde edilmesinde kullanılmıştır.
Loai Al Omari, Paul Barnes, Grant Pitman(2012)	Bilgi Teknolojileri Yönetişiminde Denetim Çabaları üzerine Keşifsel bir Çalışma: Bir Delphi Yaklaşımı (An Exploratory Study into Audit Challenges in IT Governance: A Delphi Approach)	Avustralya'nın kamu sektöründeki bilgi teknolojileri yönetişimi delphi tekniği ile deneysel bir yaklaşımla incelenmiştir.	Bilgi teknolojileri yönetişiminin denetiminin sağlanmasına yönelik olan on tane majör kaygı delphi yöntemi kullanılarak sınıflandırılmıştır.
Miklos A. Vasarheyli, Danielle Lombardi, Rebecca Bloch(2014)	Denetimin Geleceği: Uyarlanmış bir Delphi Yaklaşımı (The Future of Audit: A Modified Delphi Approach)	Denetim mesleğinin geleceği, modifiye edilmiş delphi tekniği doğrultusunda uzman görüşlerinin denetim metotlarına yönelik öngörülerinin ve düşünce yapılarının değerlendirilmesi ile incelenmiştir.	Denetim mesleğinin geleceğine yönelik tahminler ile oluşturulan önerilerde, veri tabanı yönetimi, örneklem oluşturma, genişletilebilir işaretleme dili, süreç yönetimi ve kümeleme fonksiyonları yazar tarafından ön plana çıkartılan sorumluluklar olmuştur.
Philip Davidson, Kenneth Hasledalen(2014)	Çevrimiçi Eğitime Yönelik Siber Tehditler: Bir Delphi Çalışması (Cyber Threats to Online	Çevrimiçi delphi yönteminin, delphi metodolojisinin klasik tasarımı doğrultusunda kullanılması ile çevrimiçi öğrenme sistemlerine yönelik siber tehditler ve güvenlik açıkları incelenmiştir.	Siber güvenlik risklerinin anlaşılmasında ve maliyetlerinin belirlenmesinde liderlik kavramı öncelikli faktör olarak tanımlanmıştır.

	Education: A Delphi Study)		
Daniel Smits, Jos Van Hillegersberg(2015)	Bilgi Teknolojileri Yönetişimi Olgunluğu: Delphi Metodu Kullanılarak bir Olgunluk Modeli Geliştirilmesi (IT Governance Maturity: Developing a Maturity Model Using the Delphi Method)	Hem yapısal süreçleri hem de örgüt kültürünü kapsayan bir bilgi teknolojileri yönetişim modelinin tasarımı yapılmıştır.	Bilgi teknolojisi yönetişiminin teknik tarafı için bir olgunluk modeli önerilirken, yönetsel kısımların her bir sahası için daha spesifik yetkinliklere ihtiyaç olduğu ortaya çıkmıştır.
Bilge Karabacak, Sevgi Özkan Yıldırım, Nazife Baykal(2016)	Kritik Altyapıların Siber Güvenliği için Tüzel Yaklaşımlar: Türkiye Örneği (Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey)	İlk olarak, Türkiye'nin kritik altyapıları verisi kalitatif olarak gömülü teori metodu ile analiz edilmiştir, ardından, delphi çalışması yasaların türetilmesi için altı adet uzmana uygulanmıştır ve son olarak odak grup mülakatı yapılmıştır.	Özellikle, Türkiye'nin kritik altyapısında özel sektör kapsamında rol alan çalışanların uyumluluk seviyelerinin daha ileride olduğu ortaya çıkmıştır.
Husam Haqaf, Murat Koyuncu(2018)	Bilgi Güvenliği Yöneticileri için Anahtar Yetkinlikler (Understanding Key Skills for Information Security Managers)	Delphi tekniğinin benimsenmesi ile bilgi güvenliği yönetimi rolü için gerekli olan başlıca yeteneklerin araştırılması.	Proje ve risk yönetimi, delphi metodolojisinin uygulanmasıyla, bilgi güvenliği yönetimi için anahtar sınıflar olarak kabul edilen on altı beceriden iki ana kategori olarak belirlenmiştir.
Hakan Altınpulluk, Mehmet Kesim and Gülsün Kurubacak(2020)	Açık ve Uzaktan Öğrenme Sistemlerinde Artırılmış Gerçekliğin Kullanılabilirliği: Nitel Delphi Çalışması	Açık öğretim ve uzaktan eğitim kapsamındaki ekosistemlerde artırılmış gerçekliğin fonksiyonelliğinin tanımlanarak uluslararası mevzuata uyumluluğunun ölçülmesi ile dışarıdan görünümünün tahmin	Delphi tekniği üç turdan oluşan süreçler dahilinde açık uçlu soruların ve altılı likert ölçeği ile hazırlanmış anketlerin on dört uzmana uygulanması ile kullanılmıştır.

	(The Usability of Augmented Reality in Open and Distance Learning Systems: A Qualitative Delphi Study)	edilmesi için delphi yöntemi kullanılmıştır.	

İncelenen çalışmalar ışığında, delphi yönteminin Türkiye'deki banka sektörüne uyarlanması araştırmada kullanılacak değişkenlerin, örneklem yönteminin ve içeriğinin belirlenmesi süreçleri ile devam etmiştir.

Başlangıçta değinildiği üzere, doktora tezinden türetilen bu çalışmada, iç denetçilerin siber güvenlik yönetişimi içindeki sorumluluklarının neler oldukları, yetkinliklerinin hangi ölçütlere göre değerlendirildikleri, bilgi güvenliğinin sağlanmasındaki temel unsurlar olarak gözetilen gizlilik, bütünlük ve erişilebilirlik kavramları bağlamında fonksiyonlarını nasıl sürdürdükleri, yasal çerçeve ve uluslararası standartlar bazındaki mevzuata uyumluluk kapsamındaki süreçlerde ne kadar etkin rol oynadıkları, takip ettikleri çalışma prensipleri ile organizasyonlardaki kurumsal yönetim ilkelerinin ve etik kuralların hangi ölçüde uyumlu oldukları, Türkiye'deki banka sektörü ele alınarak incelenmiştir. Bu bağlamda, elde edilen bulgular, iç denetçilerin siber güvenlik yönetişimi sisteminin sağlanmasında stratejik konuma sahip olduklarını ve özellikle yasal çevrenin ve uluslararası standartların takip edilerek, kurumların mevzuata uyumluluğunun sağlanmasında kilit rol oynadıklarını geçerli kılmaktadırlar. BDDK'nın 15 Mart 2020 tarihinde bankaların bilgi sistemlerine ve elektronik bankacılık hizmetlerine yönelik olarak resmi gazetede yayınladığı yönetmelik ile birlikte, iç denetçiler, hem bankaların organizasyonel yapıları içindeki hiyerarşik düzene hem de kendi yaptıkları işin doğası gereği bulundukları pozisyona bağlı olarak, üst yönetim ile yatay ilişkiye sahip olmaları nedeni ile bilgi teknolojileri süreçlerinin kontrolüne yönelik geliştirilecek aktivitelerde, genel müdür ve siber güvenlik yöneticileri ile etkileşimli bir yaklaşımla değer katıcı faaliyetlerde bulunma fırsatına sahip olmuşlardır. Bankalarda bilgi teknolojileri denetimlerinin etkinliğinin tutarlı olarak iyileştirilmesi için iç denetim ekiplerinin de iştirakine mutlak ihtiyaç olunduğu ve bu doğrultuda siber risklerin kontrol edilebilir düzeylerde tutulduğuna dair güvencenin kesin ve net olarak temin edilmesi gerektiği katılımcıların bildirilerinden çıkarılmaktadır. Bu bağlamda, siber güvenlik yönetimi süreçlerinde sürdürülen risk yönetimi aktiviteleri ile beraber oluşturulan güvenlik açıklarına ilişkin bulguların ve olağan dışı durumların mutlak suretle takip edilmesi, değerlendirilmesi ve üst yönetime raporlanması gerekmektedir. Bankaların kendi organizasyonel yapıları içinde sürdürülen yönetişim mekanizmalarının BDDK'nın yürürlüğe soktuğu yeni yasa ile uyumlu hale getirilerek daha etkin bir sisteme dönüştüğü ve siber güvenlik süreçlerindeki aktivitelerin daha verimli bir yaklaşımla kontrol edilmesinin sağlandığı katılımcılar tarafından özellikle vurgulanmıştır.

Kritik bilgilere erişimin kusursuza yakın olarak yetkilendirme prensibi çerçevesinde sağlanması için uygulanan kurumsal yönetim ilkelerinin ve etik kuralların ileri seviyede teknik konuları da kapsaması nedeni ile bilgi teknolojisi kapsamında denetim faaliyetleri rolünü üstlenen şahıslara ve ekiplere periyodik aralıklar ile eğitimler organize edilerek gerekli farkındalık kültürü oluşturulmalıdır. Özellikle, banka sektörünün doğası gereği büyük veri hacimleri ile gerçekleştirilen süreçlerdeki akışın ve sürekliliğin sağlanması için erişim mekanizmasının otomasyon doğrultusundaki iyileştirmelere olanak sağlayabilecek altyapı modelleri, donanımlar ve araçlar ile geliştirilmesi, risk kontrol aktivitelerinde etkinliğin artmasına destek olur. Bunlara ilaveten, bankaların, siber risklerin oluşturabileceği hasarlara karşı sigorta politikaları ile

korunmaları olanaklıdır. Ancak, sigorta yönteminin kullanılması için, siber risklerin niceliksel olarak ifade edilme kapasitelerinin iyileştirilmesi gereklidir. Ayrıca, siber risklerin hızlı bir biçimde değişmesine, gelişen teknolojilere paralel olarak geliştirilen güvenlik sistemlerinin etkinliklerine yönelik belirsizliklere ve oluşabilecek hasarın potansiyeline göre değişkenlik gösteren sigorta kapsamı arzına bağlı olarak yüksek prim bedelleri ile karşılaşılabilmektedir. Bu nedenlerden dolayı, banka sektörü gibi hassaslık derecesinin yüksek seviyelerde olduğu işkollarında siber risklere karşı sigorta önlemi alınmadan önce, risk yönetimi faaliyetleri kapsamında hata türleri ve etkileri analizi (HTEA) (failure mode and effect analysis) (FMEA) yöntemi ile risklerin ortaya çıkma olasılıkları, şiddeti ve tespit edilebilirlikleri hesaplanarak niceliksel dönüşüm sağlanabilir ve bu sayede de hasarlar sonucunda ortaya çıkabilecek belirsizliklere karşı bir öngörü geliştirilmiş olunur.

Çalışmanın bilimsel olarak taşıdığı niteliğin ileriki süreçlere taşınması açısından, bankalardaki bilgi teknolojileri denetimlerinde robotik süreç otomasyonu, yapay zeka, nesnelerin interneti, makine öğrenmesi, beşinci nesil kablosuz ağ sistemleri, sanal gerçeklik, blok zincir ve kuantum bilişimi gibi gelişmekte olan teknolojilerin hangi oranda kullanıldığı, Türkiye'deki siber güvenlik altyapısının uluslararası standartlara uygun olup olmadığı ve yerel ölçekte kullanılan yasaların hangi yönde eğilim göstermesi gerektiği araştırılarak, konuya daha geniş bir perspektiften yaklaşılabilir.

KAYNAKÇA

Al Omari, L., Barnes, P., & Pitman, G. (2012). An Exploratory Study into Audit Challenges in IT Governance: A Delphi Approach. *IT Governance, Management and Audit*, 1-12.

Altınpulluk, H., Kesim, M., & Kurubacak , G. (2020, April 2). The Usability of Augmented Reality in Open and Distance Learning Systems: A Qualitative Delphi Study. *International Council for Open and Distance Education, 12* (2), 283-307.

Calder, A. (2005). *IT Governance Guidelines for Directors.* Ely, Cambridgeshire: IT Governance Publishing.

Conway, C. (2020). *Approaches to Qualitative Research: An Oxford Handbook of Qualitative Research in American Music Education* (Vol. 1). New York: Oxford University Press.

Creswell, J. W. (2014). *Research Design: Qualitative, Quantitative, and Mixed Methods Approaches* (4 ed.). Lincoln, Nebraska: Sage.

Dalkey, N. C. (1967). *Delphi.* The Rand Corporation. Santa Monica, California: Clearinghouse for Federal Scientific & Technical Information.

Davidson, P., & Hasledalen, K. (2014). Cyber Threats to Online Education: A Delphi Study. In P. Dover, S. Hariharan, & M. Cummings (Ed.), *Proceedings of the 2nd International Conference on Management, Leadership and Governance, ICMLG 2014* (pp. 68-77). Massachusetts: Academic Conferences and Publishing International (ACPI).

Gantz, S. (2014). *The Basics of IT Audit, Purposes, Practices, and Practical Information.* Massachussets: Elsevier.

Haqaf, H., & Koyuncu, M. (2018). Understanding Key Skills for Information Security Managers. *International Journal of Information Management, 43*, 165-172.

Helmer, O. (1967). *Analysis of the Future: The Delphi Method.* The Rand Corporation. Santa Monica, California: Defense Technical Information Center.

Karabacak, B., Yıldırım, S. Ö., & Baykal, N. (2016). Regulatory Approaches for Cyber Security of Critical Infrastructures: The Case of Turkey. *Computer Law & Security Review, 32* (3), 526-539.

KPMG's Audit Committee Institute. (2017). *Is Everything Under Control? Audit Committee Challenges and Priorities 2017 Global Audit Committee Survey.*

Kurubacak , G. (2011). E-Learning for Pluralism: The Culture of E-Learning in Building a Knowledge Society. *International Journal on E-Learning, 10* (2), 145-167.

Kurubacak, G. (2007, July 1). Identify Research Priorities and Needs for Mobile Learning Technologies in Open and Distance Education: A Delphi Study. *Mobile Learning Technologies, 19* (2), 1-31.

Pickett, K. (2011). *The Essential Guide to Internal Auditing.* Chichester: British Library.

Ryder, R. D., & Madhavan, A. (2019). *Cyber Crisis Management Overcoming the Challenges in Cyberspace.* New Delhi: Bloomsbury.

Schreider, T. (2019). *Building an Effective Cybersecurity Program, 2nd Edition* (Vol. 2). Atlanta, Georgia: Rothstein Publishing.

Smits, D., & Hillegersberg, J. V. (2015). IT Governance Maturity: Developing a Maturity Model Using the Delphi Method. *48th Hawaii International Conference on System Sciences* (pp. 4534-4543). Kauai: Institute of Electrical and Electronics Engineers (IEEE).

Vasarhelyi, M. A., Lombardi, D., & Bloch, R. (2014). The Future of Audit: A Modified Delphi Approach. *Canadian Academic Accounting Association (CAAA) Annual Conference 2011* (pp. 1-31). Social Science Research Network (SSRN).