Esin Attorney Partnership.

Istanbul

Banking&Finance / Bankacılık ve Finans

Maintaining Operational Resilience in the COVID-19 Outbreak: What Should Banks Do Next?

Banks were required to adapt their operations in line with economic and social impacts of the COVID-19 outbreak. Consequently, they have taken measures such as remote working and limited physical banking. With limited physical access to banking services, a reinforced and resilient operational and internal system is essential to prevent service interruptions in services and to financially stabilize banks.

This alert concentrates on possible measures and key points to strengthen banks' operations against the pandemic's financial impacts.

Banks' Internal Systems

Information Systems

Banks must establish information systems based on the criteria set out in the Regulation on Banks' Internal Systems and Assessment of Internal Capital Adequacy (the "**Internal Systems Regulation**"), the Regulation on Banks IT Systems and Electronic Banking Services (due to enter into force in July) (the "**IT Systems Regulation**") and the Communiqué on the Principles of Banks' Information Systems Management (the "**Information Systems Communiqué**").

Accordingly, they must review and update their risk management policies on information systems.

As information system risks are closely associated with other operational risks banks may face, banks should review their current information systems policies to conserve a well-functioning operating system.

The senior management must scrutinize the improvement and update of information systems and the control mechanisms established to ensure the confidentiality of and access to data stored in information systems.

Bank must meet the minimum requirements set out in the Information Systems Communiqué and incorporate an information systems continuity plan into their business continuity plan elaborated below.

Outsourcing of Information Systems

In order to outsource information systems, the senior management must establish a surveillance mechanism to assess and manage the risks associated with outsourcing, as well as an effective relationship with the support

service providers.
In this respect, the senior management must put together a plan paving the way for uninterrupted procurement of support services and substitution of such services in case of any interruption. Banks must ensure the establishment of an adequate system enabling them to immediately start providing outsourced services on their own if the service is interrupted.

Online Banking

The importance of online banking has significantly grown due to remote working and limited physical access to branches. In order to fulfill demands for online banking, banks should ensure a solid online banking system to prevent any interruptions in the flow of work.

Pursuant to the Information Systems Communiqué, banks must ensure that they have an effective audit trail mechanism, business continuity and recovery plan.

The Information Systems Communiqué will be abolished on July 1, 2020 and the IT Systems Regulation will enter into force on the same date. For more information, please see our legal alert dated **March 18, 2020**.

Business Continuity Plan

Any interruption in the flow of business may have severe effects on banks' operations. Therefore, banks must establish a business continuity plan that would enable continuity and recovery of operations in case of an interruption. As such, banks should reconsider the following:

- **Business Impact Analysis:** The presence of a business impact analysis is essential in case of an interruption in a bank's business process or operations. In that respect, banks must consider factors that may cause possible interruptions, their possible implications on business and revise their recovery strategies, if needed.
- **Emergency and Contingency Plan:** Banks are obligated to incorporate an emergency and contingency plan to their business continuity plan. As markets are currently more unpredictable, banks may consider updating their emergency and contingency plans.

The Banking Regulatory and Supervisory Authority announced that it will re-inspect banks' business continuity plans. For more information, please see our legal alert dated **March 20, 2020**.

Risk Management

Internal Control Mechanism

Internal Control Operations: Internal control procedures constitutes a part of banks' daily operations. Banks must have written policies and implementations procedure that mainly addresses to the following:

- Control of operations.
- Control of communication channels, information systems and financial reporting systems.
- Compliance controls.

We believe banks may review these procedures to ensure their already-established systems are sufficient in handling the current economic scenario; if they are not sufficient, banks must make the necessary improvements.

Reporting: Another internal control mechanism is reporting. Banks are obligated to prepare reports concerning extraordinary conditions, suspicious transactions, breaches and general performance, and submit said reports to the senior management on a daily, weekly or monthly basis. Given the overall impact of the COVID-19 outbreak on the market, banks may consider submitting these reports to the senior management more frequently.

Control of Communication Channels and Information Systems: Through control of communication channels

and information systems, banks ensure reliable, accurate, monitorable and consistent procurement and access to information. Banks have temporarily shut down numerous branches and switched to remote working, or minimized physical banking services in terms of their number of personnel and business hours. Therefore, it is vital to have sound information channels and information systems; banks may review their communication channels and information systems, and update them if necessary.

Risk Management Systems

The objective of a risk management system is to identify, assess and control risk exposure (i.e., consolidated and unconsolidated risks, and transactional risks within the bank's risk group) through adopted policies, implementing principles and limits concerning risk-yield ratio of future cash flows.

A risk management system also contains stress test programs. Stress test programs are designed to measure financial risks and volatility that may arise due to banks-specific issues or pressured economy.
A stress test program must include the following:

- Clearly defined objectives
- Scenarios and assumptions compatible with the bank's operations and the risks associated with the operations.
- A solid methodology.
- Reporting that would support decisions taken in that regard.
- Continuous and effective review of the stress test process.
- Managerial measures to be taken in response to stress test results.

In addition to separately addressing each important risk with stress tests, a stress test that holistically assesses all of these risks must also be conducted by banks.

Stress tests concerning market risks, counterparty credit risks and collective liquidity risks must be simultaneously conducted once a month or more frequently. The Senior management is responsible for monitoring results.

Due to the economic impact and volatility of the COVID-19 outbreak, banks may need to conduct stress tests more frequently.

Measuring the Operational Risk

Pursuant to the Regulation on the Calculation and Assessment of Bank' Capital Adequacy (the "**Capital Adequacy Regulation**") banks must examine their operational risks.

Operational risk refers to the probability of incurring losses due to inadequate or unsuccessful internal systems, persons and processes or external factors.

Banks may reassess whether their operational risk management processes meet the requirements enumerated under the Capital Adequacy Regulation, in addition to the criteria set out in the Operational Risk Management Guide.

Internal Capital Adequacy Assessment Process (ICAAP)

Banks prepare an ICAAP report that covers the risk measurements, capital and liquidity plans and the risk management capacity at least once a year. The ICAAP report is prepared according to the procedures and principles set out under the ICAAP Report Guide.

Banks must continuously appraise their ICAAP report to see if they need to modify their risk measurement techniques, capital and liquidity plans and risk management capacities.

Capital and Liquidity Adequacy

Liquidity Adequacy Ratio (LAR)

The Regulation on the Calculation and Assessment of Banks' Liquidity Adequacy sets out the minimum liquidity adequacy ratio ("**LAR**") for banks.

Unless otherwise specified by the Banking Regulatory and Supervisory Board, the arithmetic average of total LAR for the first and maturity segment and the total LAR for the second maturity segment cannot be lower than 100%. Whereas, the arithmetic average of foreign currency LAR for the first and the foreign currency LAR for the second maturity segment cannot be lower than 80%.

Banks may consider continuously appraising their liquidity positions and recalculating total and foreign currency LARs to not fall short of minimum requirements set out in the Liquidity Adequacy Regulation at any time.

Capital Conservation and Countercyclical Capital Buffers

The Regulation on Capital Conservation and Countercyclical Capital Buffers (the "**Capital Conservation Regulation**") sets out the calculation method of the additional core capital ratio and measures to be taken in case a bank falls short of said ratios.

Accordingly, a bank must reserve additional capital to prevent its equity from failing to satisfy capital adequacy regulations due to credit expansion that may increase the risk in the financial sector.

In that regard, it is important for banks to continuously assess whether their additional core capital ratios are in line with the ratios and restrictions set out in the Capital Conservation Regulation. Further, banks may also review their capital conservation plans and take additional measures, if necessary.

For additional issues and measures concerning public banks, please see our client alert dated **March 27, 2020**.

Please stay up to date with further developments through the Esin Attorney Partnership Coronavirus Helpdesk.

Bankaların COVID-19 Salgınında Operasyonel Dayanıklılığı Nasıl Sağlanabilir?

Bankaların, operasyonel işleyişlerini COVID-19 salgının ekonomik ve sosyal etkileri doğrultusunda şekillendirmesi gerekince, uzaktan çalışma ve fiziksel bankacılığa erişimin sınırlandırılması gibi çeşitli tedbirler alındı. Fiziksel bankacılığın sınırlandırılması ile beraber, hizmet kesintilerini önleyebilmek ve bankaların finansal yapılarında istikrarı sağlayabilmek daha güçlü ve esnek bir operasyon ve iç sistem ihtiyacını ortaya çıkardı.

Bu bültenimizde, salgının finansal etkileri karşısında bankaların operasyonlarını güçlendirebilmek için alınabilecek olası tedbirler ile dikkat edilmesi gereken noktalar değineceğiz.

Bankaların İç Sistemleri

Bilgi Sistemleri

Bankalar, bilgi sistemlerini Bankaların İç Sistemleri ve İçsel Sermaye Yeterliliği Değerlendirme Süreci Hakkın Yönetmelik ("**İç Sistemler Yönetmeliği**"), Temmuz'da yürürlüğe girecek Bankaların Bilgi Sistemleri ve Elektronik Bankacılık Hizmetleri Hakkında Yönetmelik ("**Bilgi Sistemleri Yönetmeliği**") ile Bankaların Bilgi Sistemleri Yönetiminde Esas Alınacak İlkelere İlişkin Tebliğ'de ("**Bilgi Sistemleri Tebliği**") ve belirtilen kıstaslara uygun olacak şekilde oluşturmakla yükümlüdür.

Bu çerçevede Bankalar, bilgi sistemleri yönetimine ilişkin politikaları gözden geçirir ve ihtiyaç olması halinde günceller.
Bilgi sistemlerine ilişkin riskler, bankacılık faaliyetlerinden kaynaklanan diğer risklerin bir çarpanı olabileceği için düzgün işleyen bir operasyonel sistemin sağlanabilmesi adına güncel bilgi sistemleri politikalarının gözden

geçirilmesi gerekmektedir.

Bankaların üst yönetimi, bilgi sistemlerinin ve bilgi sistemlerinde saklanan verilerin gizli ve ulaşılabilir olması için oluşturulan kontrol altyapısının geliştirilmesi ve düzenli olarak güncellenmesi çalışmalarını gözlemlemekle yükümlüdür.

Bankalar, bilgi sistemleri servislerinin sürekliliğini sağlayabilmek adına aşağıda açıklanan iş sürekliliği yönetimi planının bir parçası olarak bilgi sistemleri süreklilik planını oluşturmakla yükümlüdür.

Bilgi Sistemleri İçin Destek Hizmeti Alımı

Bankaların üst yönetimi, bilgi sistemleri için alınacak destek hizmetinin banka açısından doğuracağı riskleri değerlendirmek, yönetmek ve destek hizmeti kuruluşu ile ilişkilerin etkin bir şekilde yürütülmesine olanak sağlamak için bir gözetim mekanizması tesis eder.

Bu çerçevede, üst yönetimin destek hizmetinin kesintisiz olarak sağlanması ve hizmette kesinti olması durumunda, hizmetin ne şekilde ikame edilebileceğini öngören bir planının olması gerekmektedir. Bu çerçevede bankaların, bilgi sistemlerine ilişkin destek hizmetinde kesinti olması halinde, hizmeti gecikmeden kendilerinin sağlayabilecekleri bir mekanizmaya ihtiyaçları olacaktır.

Dijital Bankacılık

Dijital bankacılığın önemi, evden çalışma sistemine geçilmesi ve fiziksel bankacılığın sınırlandırılması ile birlikte epey artmıştır. Bankaların, dijital bankacılığa karşı oluşan yoğun talebin karşılanabilmesi adına, dijital bankacılık hizmetlerinin kesilmesini önleyecek güçlü bir dijital bankacılık sistemi kurması gerekmektedir.

Bilgi Sistemleri Tebliği uyarınca bankalar etkin bir denetim izi tutma mekanizması ile servis sürekliliği ve kurtarma planına sahip olmalıdır.

Bilgi Sistemleri Tebliği 1 Temmuz 2020'de yürürlükten kalkacak ve yine aynı tarihte Bilgi Sistemleri Yönetmeliği yürürlüğe girecektir. Bu konuda daha detaylı bilgi için **18 Mart 2020** tarihli mevzuat duyurumuza başvurabilirsiniz.

İş Sürekliliği Planı

İş sürekliliğindeki herhangi bir aksaklık bankanın operasyonlarında önemli, olumsuz etkiler yaratabilir. Olası bir kesinti durumunda bankanın faaliyetlerinin sürdürülebilmesi için iş sürekliliği planının oluşturulması zorunludur. Bu nedenle bankaların aşağıda belirtilen hususları gözden geçirmesi büyük önem arz etmektedir:

- **İş Etki Analizi:** Bankanın kesinti sebebiyle faaliyetlerini sürdüremediği hallerde iş etki analizinin bulunması önem arz etmektedir. Bu kapsamda bankalar, iş sürekliliğinde kesintiye sebep olabilecek olası nedenler ile bu nedenlerin faaliyetlerinde yaratacağı olası etkileri değerlendirmeli ve gerekmesi halinde kurtarma stratejilerini güncellemelidir.
- **Acil ve Beklenmedik Durum Planı:** Bankalar, iş sürekliliği planlarının bir parçası olarak acil ve beklenmedik durum planı oluşturmak zorundadır. Piyasadaki artan belirsizlik dikkate alındığında, bankaların acil ve beklenmedik durum planlarını güncellemeleri gerekebilir.

Bankacılık Düzenleme ve Denetleme Kurumu bankaların iş sürekliliği planlarını yeniden gözden geçireceğini duyurmuştur. Söz konusu açıklamaya ilişkin detaylı bilgi için **20 Mart 2020** tarihli mevzuat duyurumuza başvurabilirsiniz.

Risk Yönetimi

İç Kontrol Sistemi

İç Kontrol Faaliyetleri: İç kontrol faaliyetleri bankanın günlük faaliyetlerinin bir parçasını oluşturur. Bankaların oluşturduğu yazılı politika ve uygulama prosedürlerinin aşağıdaki hususları düzenlemesi gerekir:

- Faaliyetlerin icrasına yönelik işlemlerin kontrolü.
- İletişim kanallarının, bilgi sistemlerinin ve finansal raporlama sistemlerinin kontrolü.
- Uyum kontrolleri.

Bankaların, önceden oluşturulan bu politikaların güncel ekonomik durum ile uyumlu olup olmadığının gözden geçirmesi ve politikalar uyumlu değilse gerekli düzeltmelerin yapılması gerekmektedir.

Raporlama: İç kontrol faaliyetlerinden bir diğeri de raporlamadır. Bankalar, üst yönetime sunmak üzere günlük, haftalık veya aylık bazda olağanüstü durum, şüpheli işlem, aykırılık ve genel performansa ilişkin rapor hazırlamakla yükümlüdür. COVID-19 salgınının ekonomideki genel etkisi düşünüldüğü zaman söz konusu raporlamaların daha sık aralıklarla yapılması düşünülebilir.

İletişim Kanallarının ve Bilgi Sistemlerinin Kontrolü: Bankanın iletişim kanallarının ve bilgi sistemlerinin kontrolü ile banka bünyesinde elde edilen bilginin güvenilir, tam, izlenebilir ve tutarlı biçimde olması ve bilgiye erişimin sağlanması amaçlanmaktadır. Bankalar, geçici olarak pek çok şubesini kapatarak evden çalışma sistemine geçmiş veya fiziksel bankacılık hizmetini çalışan personel ve çalışma saatleri bakımından sınırlandırmıştır. Bu nedenle bankaların güçlü iletişim kanalları ve bilgi sistemlerini kurmuş olmaları önem arz etmektedir. Bu kapsamda söz konusu iletişim kanalları ile bilgi sistemlerinin gözden geçirilmesi ve gerekmesi halinde bunları güncellemeleri yararlı olacaktır.

Risk Yönetimi Sistemi

Risk yönetimi sisteminin amacı, bankanın maruz kaldığı riskin (konsolide ve konsolide olmayan bazda maruz kalınan riskler ile bankanın dahil olduğu risk grubu ile gerçekleştirilen işlemlerden kaynaklanan risklerin), bankanın gelecekteki nakit akımlarının barındırdığı risk-getiri yapısına yönelik oluşturulan politikalar, uygulama usulleri ve limitler vasıtasıyla tanımlanması, ölçülmesi, raporlanması, izlenmesi ve kontrolünün sağlanmasıdır.

Bankanın risk yönetim sürecine stres testi programları da dâhildir. Stres testi, bankaya özgü olumsuz gelişmelerden kaynaklanabilecek veya stres altındaki ekonomik ve finansal ortamda ortaya çıkabilecek finansal risk fve kırılganlıkların ölçülmesi amacıyla geliştirilir.

Stres testi programı aşağıdaki unsurları barındırmalıdır:

- Açıkça tanımlanmış amaçlar.
- Bankanın faaliyetleri ve bu faaliyetlerden kaynaklanan risklerle uyumlu tasarlanmış senaryo ve varsayımlar.
- Güçlü bir stres testi yöntemi.
- Alınan kararları destekleyecek raporlamalar.
- Stres testi süreçlerinin devamlı ve etkin bir şekilde gözde geçirilmesi.
- Stres testi sonuçlarına dayalı yönetim aksiyonları.

Bankalar, her bir önemli risk bazında stres testi yapmanın yanı sıra, bu risklerin tümünün dikkate alındığı genel stres testlerini de yapmakla yükümlüdür.

Piyasa ve karşı taraf kredi riski ile bankanın toplam likidite riskine ilişkin yapılacak stres testleri eş zamanlı olarak ayda bir veya daha sık periyotlarla tekrarlanır. Stres testi sonuçlarının takibi banka üst yönetimine aittir.

Bankalar, COVID- 19 salgınının ekonomik etkileri ve ekonomideki dalgalanmalar nedeniyle daha sık stres testi yapılması gerekebilir.

Operasyonel Riskin Ölçülmesi

Bankalar, Bankaların Sermaye Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik ("**Sermaye Yeterliliği Yönetmeliği**") uyarınca operasyonel risklerini ölçmek durumundadır.

Operasyonel risk; yetersiz veya başarısız iç süreçler, insanlar ve sistemlerden ya da harici olaylardan kaynaklanan zarar etme olasılığını kapsamaktadır.

Yukarıdaki bilgiler kapsamında bankalar, operasyonel risk yönetimine ilişkin sürecin Sermaye Yeterliliği Yönetmeliği ve Operasyonel Risk Yönetimine İlişkin Rehber'de yer alan gereklilikleri yerine getirip getirmediği hususunu gözden geçirebilir.

İçsel Sermaye Yeterliliği Değerlendirme Süreci (İSEDES)

Bankalar yapılan risk ölçümünü, sermaye ve likidite planlaması ile risk yönetim kabiliyetlerine ilişkin değerlendirmeyi kapsayan İSEDES raporunu yılda en az bir kere hazırlar. İSEDES raporu hazırlanırken, İSEDES Raporuna İlişkin Rehber'de belirlenen usul ve esaslar dikkate alınmalıdır.

Bankalar; risk ölçümü, likidite planlaması ve risk yönetim kabiliyetlerinde bir değişiklik yapılmasının gerekli olup olmadığını değerlendirebilmek adına İSEDES raporlarını devamlı olarak gözden geçirmelidir.

Sermaye ve Likidite Yeterliliği

Likidite Yeterlilik Oranı

Bankaların Likidite Yeterliliğinin Ölçülmesine ve Değerlendirilmesine İlişkin Yönetmelik'te ("**Likidite Yeterliliğine İlişkin Yönetmelik**"), bankaların sağlaması gereken asgari likidite yeterliliği oranı düzenlenmektedir.

Bankacılık Düzenleme ve Denetleme Kurulu tarafından farklı bir oran kararlaştırılmadığı takdirde, bankların birinci vade dilimine ilişkin toplam likidite yeterlilik oranlarının haftalık basit aritmetik ortalaması ile ikinci vade dilimine ilişkin toplam likidite yeterlilik oranı yüzde yüzden az olamaz. Birinci vade dilimine ilişkin yabancı para likidite yeterlilik oranı ile ikinci vade dilimine ilişkin yabancı para likidite yeterlilik oranı ise yüzde seksenden az olamaz.

Bankalar, Likidite Yeterliliğine İlişkin Yönetmelik'te belirlenen asgari likidite yeterliliği oranını sürekli olarak sağlayabildiklerinin tespiti için likidite durumlarını devamlı olarak inceleyebilir ve bu kapsamda toplam ve yabancı para likidite yeterlilik oranlarını yeniden hesaplayabilir.

Sermaye Koruma ve Döngüsel Sermaye Tamponlarına İlişkin Yönetmelik

Sermaye Koruma ve Döngüsel Sermaye Tamponlarına İlişkin Yönetmelik ("**Sermayenin Korunması Yönetmeliği**"), sermaye koruma tamponu ve ilave çekirdek sermaye tutarının hesaplanması ile ilave çekirdek sermaye gereksiniminin karşılanamaması halinde alınacak tedbirleri düzenlemektedir.

Bu kapsamda, finansal sektörün genel risk düzeyinin kredi genişlemesi sonucu artması ve bunun sonucunda özkaynakların sermaye yeterliliğine ilişkin düzenlemeler karşısında yetersiz kalmasının engellenmesi amacıyla belli bir ilave çekirdek sermaye tutarı bulundurulması zorunludur.

Bankaların ilave çekirdek sermaye tutarının Sermayenin Korunması Yönetmeliği'nde belirtilen oran ve sınırlar dâhilinde olup olmadığının devamlı değerlendirilmesi faydalı olacaktır. Buna ek olarak, bankalar gerekmesi halinde sermaye koruma planlarını da gözden geçirebilirler.

Halka açık bankaların uyması gereken ek yükümlülükler için **27 Mart 2020** tarihli mevzuat duyurumuza başvurabilirsiniz.

COVID-19 salgını kapsamında atılan hukuki adımlarla ilgili detaylar için Koronavirüs Masamız'a başvurabilirsiniz.