შპს ქართულ-ამერიკული უნივერსიტეტი

Georgian American University, LLC

ბიზნესის სკოლა

Business School

დავით პაპუაშვილი

David Papuashvili

კიბერრისკები და შიდა კონტროლის მექანიზმები ფინანსურ სისტემაში

Cyber Risk and Internal Control Mechanisms in the Financial System

წარდგენილია ბიზნესის ადმინისტრირების დოქტორის აკადემიური ხარისხის მოსაპოვებლად

Submitted in Fulfillment of the Requirements for the Degree of Doctor of Philosophy in Business Administration

თბილისი, 0160, საქართველო

Tbilisi, 0160, Georgia

2023

Thesis Topic: Cyber Risk and Internal Control Mechanisms in the Financial System

As the author of the submitted work, I hereby declare that this submission is my own work and to the best of my knowledge it contains no materials previously published, accepted for publication or written by another person, or substantial proportions of material that have been accepted for the award of any other degree or diploma, except where due acknowledgement is made in the dissertation.

David Papuashvili

I would like to express my sincere gratitude and appreciation to my mentor Dr. Teimuraz Toronjadze and Dr. Aquiles Almansi for their invaluable support and guidance throughout the years.

Contents

List of Figures

List of Tables

Abstract

Cyber risk is a systemic operational risk[1]. On August 8, 2008 cyber-attacks began to affect the nation of Georgia, which went in parallel with the Russian Invasion of Georgia. Despite the fact that the most affected sector of Georgia was the public sector and telecommunications, the financial sector became a significant victim of the cyber-campaign. To offer an example, the central bank's webpage was hacked and the official exchange rate was modified by unauthorized entities. In addition, online banking services were offline for approximately 10 days due to the persistent distributed denial-of-service (DDoS) attacks that were affecting the availability of critical systems, including those that were offering information and telecommunications services.

From a financial risk perspective, according to various estimates, cybercrime alone, excluding the risk associated with system disruptions and technological failure, is to cost the global economy around $10.5 trillion annually by the year 2025.[2] While this figure is a general estimate and includes different sectors of the economy, the financial system is a prime target of cybercrime crime and a significant portion of these financial losses is incurred by the financial system. Additionally, the average cost of a cyber-attack is approximately 2.4 million US Dollars. It is also worth noting that cybercrime costs more to the financial sector than any other sector of the economy.

Cyber risk has become key to most business operations today, since information technology is often an enabler and a critical supporting process. Many companies, including financial institutions, still have not adjusted their processes adequately to manage cyber risk. Research shows that cyber and IT risks arise not from technical or people-related issues at the lower level, but from a failure in governance and managerial (internal control) processes. As a result, cyber risk

[1] See Cyber Resilience Implications for the Financial System for a detailed review of the systemic implications of cyber risk.
[2] Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/

should be managed in such a manner, as to ensure the safe and sound functioning of financial institutions.

The following research paper outlines the main components of an effective control structure to mitigate cyber risk within the financial system. The document covers the implementation of preventive, detective and corrective controls that can address some of the current and pressing issues in the area of cybersecurity from a financial systems perspective. The topics that are covered include cyber resilience, which has become an important emerging topic, business continuity, incident response, outsourcing, as well as stress testing and information sharing. The abovementioned components form the foundation of contemporary cyber risk management.

აბსტრაქტი

კიბერრისკი წარმოადგენს სისტემური მნიშვნელობის საოპერაციო რისკს. საქართველოს კერძო და საჯარო ინფრასტრუქტურაზე დიდი ზეგავლენა იქონია იმ კიბერშეტევების ჯაჭვმა, რომელიც 2008 წლის 8 აგვისტოს დაიწყო. მიუხედავად იმისა, რომ მოცემული კიბერშეტევების ძირითად სამიზნეს საჯარო სექტორი და ტელეკომუნიკაციების სფერო წარმოადგენდა, კიბერშეტევების მნიშვნელოვანი მსხვერპლი და სამიზნე ქვეყნის ფინანსური სექტორიც გახდა. მაგალითად, ქვეყნის ცენტრალური ბანკის ვებ გვერდი ჰაკერების მიერ გატყდა, სადაც, დროებით, უნებართვოდ შეიცვალა ვალუტის ოფიციალური გაცვლითი კურსი. დამატებით, ონლაინ (ინტერნეტ) საბანკო მომსახურება ქვეყნის მასშტაბით მიუწვდომელი იყო 10 დღის მანძილზე, იმ დროისათვის მიმდინარე მომსახურების შეფერხების(ე.წ. DDoS) კიბერშეტევების გამო.

ფინანსური რისკის თვალსაზრისით, სხვადასხვა მონაცემების მიხედვით, კიბერდანაშაული გლობალური ეკონომიკისთვის 10.5 ტრილიონი ა.შ.შ. დოლარის დანაკარგს მიაღწევს 2025 წლისთვის. მიუხედავად იმისა, რომ მოცემული დანაკარგის მაჩვენებელი გარკვეულ ვარაუდს წარმოადგენს და მოიცავს ეკონომიკის სხვადასხვა სფეროს, ფინანსური სისტემა კიბერშეტევების ერთერთი ძირითადი სამიზნეა. დამატებით, კიბერშეტევის საშუალო ხარჯი დაახლოებით 2.4 მილიონ ა.შ.შ. დოლარს წარმოადგენს. აღსანიშნავია ისიც, რომ კიბერდანაშაული ფინანსურ სექტორს უფრო ძვირი უჯდება ვიდრე ეკნომიკის რომელიმე სხვა სექტორს.

დღეისათვის, კიბერრისკი საყურადღებოა ბიზნეს-სექტორის ძირითადი ნაწილისთვის, რადგან საინფორმაციო ტექნოლოგია მსხვილ, გარდაუვალ და მნიშვნელოვან მხარდამჭერ როლს თანამაშობს სხვადასხვა ორგანიზაციის ყოველდღიურ ოპერაციებში, მათ შორის საკვანძო და კრიტიკული ბიზნეს პროცესების განსახორციელებლად. ამავდროულად, მრავალ კომპანიაში, ფინანსური დაწესებულებების ჩათვლით, ბიზნეს პროცესები არ არის სათანადოდ გარდაქმნილი და ჩამოყალიბებული იმ

ფორმით, რომ ორგანიზაცია გაუმკლავდეს და მართოს არსებული თუ მოსალოდნელი კიბერრისკები. არაერთმა კველვამ აჩვენა, რომ კიბერ და საინფორმაციო ტექნოლოგიური რისკები წარმოიშობა არა ტექნიკური ხასიათის ხარვეზებისგან და ორგანიზაციის საოპერაციო დონის თანამშრომლებისგან, არამედ მმართველობითი პროცესების ჩავარდნისგან და შიდა კონტროლის მექანიზმების ნაკლებობისგან. შედეგად, შეგვიძლია დავასკვნათ, რომ კიბერრისკი უნდა იმართებოდეს იმ ფორმით, რომ ორგანიზაციებმა, ფინანსური დაწესებულებების ჩათვლით, უზრუნველყონ სხვადასხვა ბიზნეს პროცესის სანდო და უსაფრთხო ფუნქციონირება.

მოცემული ნაშრომი იკვლევს, მიმოიხილავს და ხაზს უსვამს ეფექტური კონტროლის მაქნიზმების აუცილებლობას ფინანსურ სისტემაში არსებული კიბერრისკის შესარბილებლად. თეზისი განიხილავს პრევენციული/შემაკავებელი, აღმოჩენითი და მაკორექტირებელი კონტროლების ერთობლიობას მიმდინარე საფრთხეებისა თუ რისკების სამართავად, ფინანსური სისტემის ჭრილში. ამავდროულად, ძირითადი ყურადღება მახვილდება კიბერ-მედეგობის, როგორც კიბერუსაფრთხოების ერთერთი ამომავალი საკითხის, ბიზნეს უწყვეტობის, ინციდენტებზე რეაგირების პროცესის, აუთსორსინგის, სტრეს-ტესტირებისა და ინფორმაციის გაცვლის მართვის მექანიზმებზე. ზემოაღნიშნული მიმართულებები და შესაბამისი კონტროლის მექანიზმები ქმნის იმ ფუძეს, რომელზეც უნდა დაშენდეს კიბერრისკის თანამედროვე მართვის პროცესი.

Introduction

In August of 2008, cyber-attacks began to affect the Georgian public and private sectors. The cyber-attacks coincided with the Russian Invasion of Georgia, which is also known as the “Five-Day War”. While most of the initial cyber-attacks that were directed against Georgia affected the public sector and media, including various government websites and Georgian news portals, a significant portion of the cyber-attacks affected the Georgian financial system[3].

The cyber-attacks that were directed at the financial system had the effect of bringing down online banking services. In addition, the National Bank of Georgia, which serves as the central bank of Georgia, had its website hacked. As a result of the hack, the official, reference exchange rate of the Georgian Lari to the U.S. Dollar was modified. Luckily, most consumers and other stakeholders were unable to see the unauthorized modification of the exchange rate due to the fact that most of the Georgian internet space was under a distributed denial-of-service attack at the time. If the exchange rate modification on the central bank’s webpage would have been seen by a larger audience, when Internet services are generally readily available to the public, the implications and the impact to the financial system would likely have been much greater.

The events of August, 2008 and several other large-scale cyber risk-related incidents illustrate that cybersecurity and cyber resilience have become an increasingly vital part of financial stability. In addition, the growing use and adoption of electronic information systems in the face of digital transformation of the financial system has clearly brought cyber risk to the forefront of attention.

According to the U.S. National Institute of Standards and Technology (NIST), **cyber resilience** is defined *as the ability to anticipate, withstand, recover from, and adapt*

[3] Papuashvili, D. (2023). Cyber Resilience Implications for the Financial System. Business Administration Research Papers. Retrieved from https://barp.openjournals.ge/index.php/barp/article/view/6774

to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources[4]. Financial institutions that make up the financial system, especially those institutions that are deemed as being systemically important to the safe and sound functioning of the economy, need to have credible and effective control mechanisms in order to mitigate cyber risk. This includes relevant governance, management and other control processes in order to ensure cyber resilience. Furthermore, cybersecurity also needs to include an aspect of stress testing in the wake of adverse or unexpected events. Without a robust stress testing framework, it will be difficult to gain assurance that an organization such as a commercial bank or a credit union will be able to cope with various cyber risk scenarios. It is therefore important to have a holistic approach towards cyber resilience and cyber risk, in general. This is especially true for the financial system, since it forms the backbone of most national economies.

The following paper presents and discusses various aspects of cybersecurity, including the implementation of internal controls that are vital for the safe and sound functioning of financial institutions.

Cyber Risk as Financial Risk

Cyber risk is a form of operational risk. Operational risk is defined as the risk of loss arising from failed or inadequate processes, people, systems, external events[5]. Cyber risk is also clearly a form of information technology risk, which is itself a subset of operational risk.

While operational risk is mostly viewed as a form of non-financial risk, since in many cases, operational risk's impact on the organization is not as clearly defined in financial terms as those of credit, or market risk, there are several forms of operational risk that have tangible financial implications. This includes the risk of fraud, which can lead to both direct and indirect financial loss, and cyber risk,

[4] Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. & Guissanie, G. (February, 2020). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

[5] Basel Committee for Banking Supervision (BCBS).

which also can be linked to fraud and which may have various adverse financial consequences for financial institutions.

IT risk, which is often linked directly to cyber risk, is the likelihood for an unplanned event involving a system failure or business disruption in information technology to negatively affect an organization's business objectives.[6] Information technology risk is a business risk. Therefore, if cyber risk is viewed as a subset of information technology risk, it is also clearly a form of business risk, with financial implications.

Cyber Risk and Operational Risk

Cyber risk has become key to most business operations today, since information technology is often an enabler and a critical supporting process. Many companies, including financial institutions, still have not adjusted their processes adequately to manage cyber risk. Research shows that IT risks arise not from technical or people-related issues at the lower level, but from a failure in governance and managerial (internal control) processes. As a result, cyber risk should be managed in such a manner, as to ensure the safe and sound functioning of a financial institution.

Cyber risk is more likely to be realized with systemic consequences than other forms of operational risk. This makes cyber risk a unique form of operational risk, which can spread through the system at much greater speeds, affect multiple organizations at the same time and also lead to financial losses. The impact of cyber risk has also been studied less than both other forms of financial and operational risk. As a result, it is not fully clear what the exact financial impact might be when a hacker deliberately modifies the official currency exchange rate, or the interest rate of a key monetary policy instrument[7]. Furthermore, if a financial institution's data integrity is compromised, it might be difficult to assess how a bank might be able to service its customers. Additionally, if access to client funds is impaired due

[6] Westerman, G. & Hunter, R. (2007). IT Risk: Turning Business Threats into Competitive Advantage.

to a cyber-attack at one commercial bank, this might also cause systemic risk implications, if customers lose trust in the viability of other financial institutions to provide basic financial services.

From a financial risk perspective, according to various estimates, cybercrime alone, excluding the risk associated with system disruptions and technological failure, is to cost the global economy around $10.5 trillion annually by the year 2025.[8] While this figure is a general estimate and includes different sectors of the economy, the financial system is a prime target of cybercrime crime and a significant portion of these financial losses is incurred by the financial system. Additionally, the average cost of a cyber-attack is approximately 2.4 million US Dollars. It is also worth noting that cybercrime costs more to the financial sector than any other sector of the economy. Furthermore, Cybercrime costs more to the financial sector than any other sector. The number of successful attacks has increased by approximately 3 times in the last several years. Figure 1 below depicts the cyber threat landscape for the financial market infrastructures in Europe. As can be clearly determined from the diagram, the motivation of the various threat sectors is clearly financial as evidenced by the threat of extortion, financial gain and financial data theft. In terms of the main threats that the European financial market infrastructure faces, top threats such as ransomware-encryption and data theft mostly have financial implications as an end-result, since hackers and other unauthorized parts usually either extort money from affected victim institutions, or execute cyber-attacks with the aim of financial gain.

Operational Risk Management Framework

Since cyber risk is a key form of operational risk, it makes considerable sense to include cyber risk within a financial institution's overall operational risk management framework. The operational risk management (ORM) framework, should at a minimum include:

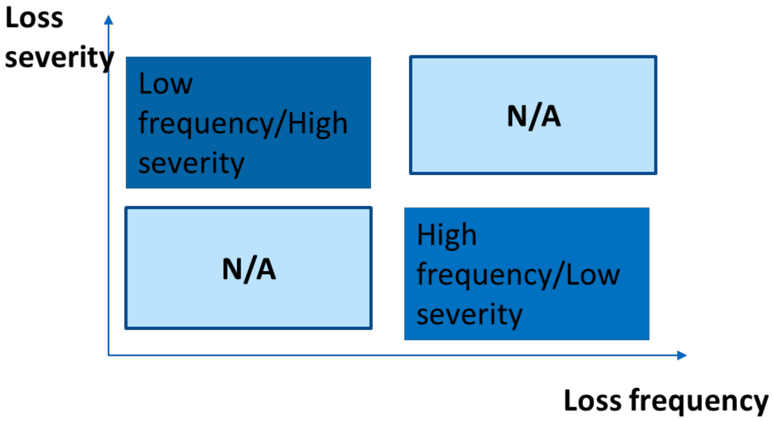
[8] See Morgan's review of the topic for further reference.

- Definition of operational risk and operational loss
- Monitoring and Reporting of Risk
- loss data gathering processes and methodology
- Contingency/business continuity planning
- Internal control mechanisms
- outsourcing risk management
- Fraud prevention policy
- information security management
- Data quality management and accuracy risk

These components mentioned above are vital for the effective management of operational risk that also includes cyber risk. Additionally, without a credible definition of what constitutes operational risk, it will be challenging and difficult to identify the role of cyber risk within the operational risk management framework.

The objective of operational risk management is to prevent operational losses, especially large losses. Large operational risk events are mostly due to fraud, which can arise from cyber risk-related events, such as unauthorized financial transactions (i.e. Bank of Bangladesh unauthorized transfers). In addition, the main goal of operational risk management is to lower the frequency and severity of large-loss events. The primary challenge for operational risk management is to ensure a low frequency of major events (high severity) that can cause large losses. Figure 1 below depicts the kind of operational risk that organizations should concentrate on. The realistic approach of managing cyber risk (within the confines of operational risk management) is to concentrate on low-severity, high-frequency events, as well as low-frequency, high-severity events as described in the diagram below[9].

Figure 1. Operational and Cyber Risk Supervision and Loss Event Classification. What should the risk managers concentrate on?



Source: *Chernobai, Rachev and Fabozzi*

Other aspects to consider for cyber risk management include some of the universally applicable operational risk management initiatives. These principles specifically stress the need to increasing risk awareness within organizations, adopting a proactive risk analysis process (as oppose to reactive risk analysis), using risk-based performance measurements, Improving operational efficiency, implementing system changes to control processes, and putting operational limits in place. The Basel Committee for Banking Supervision Recommends that banks use a standardized taxonomy for operational risk management. This would include the mapping of a bank's business lines as well as the classification of losses into specific loss event categories. Operational risk management will not be effective if a bank's employees have different understanding of operational risk terms. An example would be when a bank's risk officer has a different understanding of fraud compared to an accountant. It is therefore very important for all of the employees

[9] Nadirashvili, K., Papuashvili, D., Razmadze, R. (2020). Quantitative Risk Assessment Approaches to Operational Risk Management. Journal "Economics and Banking" (Georgian). Volume 7. Tbilisi, Georgia.

of the financial institution to be using the same lexicon of operational risk terminology

Another important aspect to consider is the establishment of a reporting framework in addition to other key features such as contingency planning. From the perspective of contingency planning, the following key questions need to be answered:

- What is the degree of protection provided by a bank's contingency plan against major unexpected events affecting the bank?
- ◆ What is the time it would take to recover from an event and return to normal operations?
- ◆ What is the cost and adaptability of the continuity plan to changes in resources and processes?

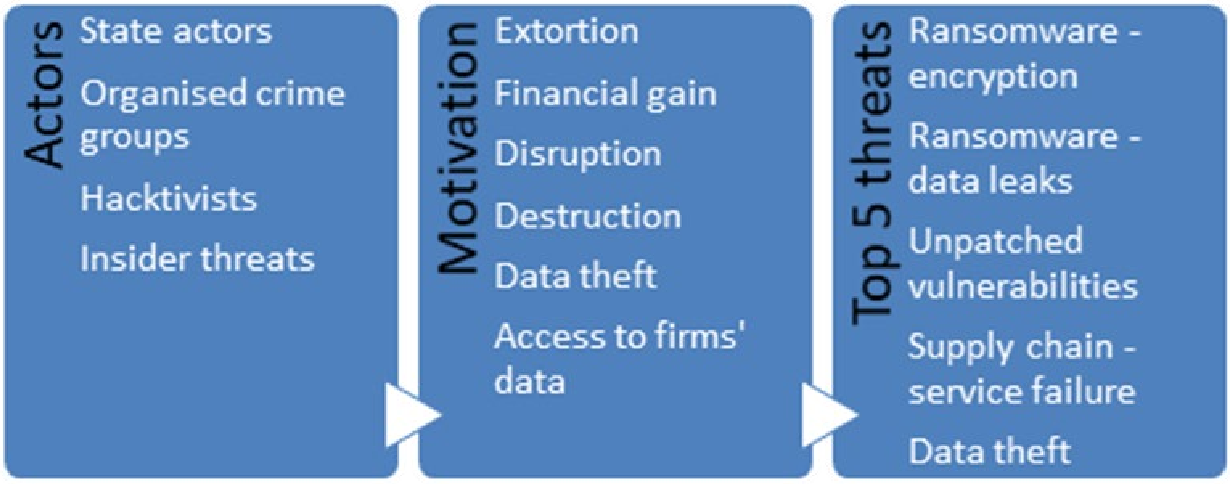
It is also worth noting that external operational failures are far harder to control and require comprehensive contingency plans. Cyber-attacks can bring down a bank's internet-based operations to offer but one example. Another point for consideration is that the quality of a contingency plan is directly proportional to the time and effort that staff have put into developing the plan. The challenge also lies in the fact that if risk managers do not take into consideration some of the relevant unexpected risks, the contingency plan may not be effective.

An organization that has a strong operational management framework and relevant effective controls might be characterized by the following:

- A high level of awareness of operational risk by the risk management, including executive management.
- Dedicated, independent operational risk management function and Committee/s

- Realistic policies and procedures for all important areas of operational risk that are understood and used by staff.
- Strategy for the development of information technology fully meets the requirements of the business of the Bank
- The effective use of management information systems throughout the organization including reporting to the risk management.
- Strong preventive, detective and corrective controls in place across the entire IT environment.
- Effective management of operational issues including, outsourcing operations, new products, project management and fraud.
- Strong business continuity and disaster recovery plans and procedures in place that are frequently tested.
- Minimal findings from independent reviews (including internal/external audit functions) of key operational risk areas.

Figure 2. Cyber threat landscape for financial market infrastructures in Europe



Note: Threats are arranged in descending order of estimated severity.

Source: European Central Bank

Cyber Resilience

Executive and senior management of financial institutions need to be responsible for setting the tone at the top for cyber resilience processes. If the organization's employees perceive that there is a lack of interest and initiative from the part of executive management, it will be very difficult and challenging to implement an effective cyber resilience framework within the organization. The executive management of a financial institution is the one that is responsible for establishing the cyber resilience framework and making sure that cyber risk is effectively managed. The executive management is also responsible for setting the relevant risk tolerance for cyber risk. The cyber resilience framework should be based on a widely accepted standard or framework that can be independently verified and assessed by relevant entities, such as external audit. For example, the cyber resilience framework can be based on the NIST framework, as advocated by the Basel Committee for Banking Supervision (BCBS) and include the five main functions of asset identification, protection, detection and incident response.

An effective cyber and IT risk management framework needs to include a specific set of objectives and a relevant strategy, the aim of which is to implement the objectives that have been established by management. The various management bodies/persons of the financial institution should have respective responsibilities, the main points of which are presented below.

An effective information technology risk management and cyber resilience framework should classify information technology risk losses by loss event type. Executive management of the organization should therefore take the lead in establishing a strong risk management culture, develop a management culture, and supporting processes, to understand the nature and scope of the information technology risk inherent in the institution's strategies and activities, and develop comprehensive, dynamic oversight and control environments that are fully integrated into or coordinated with the overall framework for managing all risks across the whole organization.

It is also important to note that the organization should implement a code of conduct or an ethics policy that sets clear expectations for integrity and ethical values of the highest standard and identify acceptable business practices for all of the employees of the organization. Executive management should also approve and periodically review policies comprehensively and appropriately documenting the IT risk management framework. A risk appetite and tolerance statement for IT and other operational risk areas that identifies the nature, type and levels of information technology risk that the organization is willing to assume need to be developed.

Furthermore, the executive management needs to oversee and supervise senior management in order to ensure that the policies, processes and systems are implemented effectively at all levels of the organization, including the operational level. Last, but not least, the executive management should also ensure that the institution's cyber risk management framework, including the cyber resilience framework is subject to effective independent review by audit or other appropriately trained parties.

Other key areas that the senior management is responsible for is to ensure that bank activities are conducted by staff with the necessary experience, technical capabilities and access to resources. Staff responsible for monitoring and enforcing compliance with the institution's risk policy should have authority independent from the units they oversee. In addition, senior management should maintain an effective issue-resolution processes. This process should generally cover and include a reporting process to track and, when necessary, escalate issues in order to make sure that issues are addressed and resolved.

There should also be a mechanism that is set up to implement a process to regularly monitor cyber risk, within the context of an overall operational risk management framework. Material operational losses associated with cyber risk should be recorded and analyzed. Again, in this respect, senior management should make sure that an appropriate level of cyber risk training is available at all levels of the organization. This process should also cover cyber resilience processes and the training that is provided should reflect the seniority, role and responsibilities of the individuals for whom it is intended. Senior management should implement business resiliency and continuity plans.

Internal Control

Internal controls are measures that banks can implement to spot or determine risk exposures and prevent them from turning into loss events. Risk managers should make sure that banks and other financial institutions have effective internal controls that match the size and complexity of the operations, risk appetite and tolerance. Examples of an internal control include limits on loan approvals Key risk indicators (KRIs) are commonly used within the system of internal controls. Two common internal controls include detective controls and preventive controls. Detective controls alone, do not limit losses, but can alert a bank to a potential risk exposure. Preventive controls are more proactive. Examples of preventive controls include withdrawal Limits on ATM cards and PIN numbers.

A key consideration to emphasize is that itt is better to manage operational risk, including cyber risk in a proactive, instead of a reactive manner. This is due to the fact that in certain cases, “reacting” to a significant cyber risk event, such as a system disruption or a cyber-attack may be too late and either the financial institution (such as a bank), or even the financial system may not be able to fully recover from such an event.

Cyber risk management should include the assessment of both inherent risk, as well as the quality of information technology risk management and internal controls. Inherent risk for information technology is the exposure to a specific technology risk, in the absence of any control mechanism being applied. In terms of the quality of information technology risk management and internal controls, the risk manager must assess how information technology risk is being managed within a financial institution. Specifically the quality of management oversight for information technology risk, as well as the relevant control mechanisms in the form of preventive, detective and corrective controls needs to be examined by the risk manager. This aspect is an important element in assessing the overall risk profile of the bank or other financial institutions.

Information Technology Risk and Cyber Risk

Cyber risk is often viewed within the prism of information technology (IT) risk. As has already been noted, IT risk is the likelihood for an unplanned event involving a system failure or business disruption in information technology to negatively affect an organization's business objectives.[10] Information technology risk is a business risk. It is no longer confined to an organization's information technology department Information technology risk is a key operational risk that can have significant implications for the business. IT has become key to most business operations today, since it is often an enabler and a critical supporting process. Many companies, including financial institutions, still have not adjusted their processes adequately to manage IT risk. Research shows that IT risks arise not from technical or people-related issues at the lower level but from a failure in governance and managerial (internal control) processes. The connection can be made here that cyber risk, which is closely associated with IT risk also arises from a lack of effective governance and relevant internal control mechanisms. Annex 1 provides a cyber risk self-assessment checklist which can be used by risk practitioners to assess the level and quality of cyber risk management within the organization.

Risk-based Considerations for Cyber Risk Management

Cyber risk management should be forward-looking. Since information systems and the associated technology and processes are constantly changing, it is highly recommended that cyber and IT risk management be principles-based, as opposed to a rules-based regime. Annex 2 describes a few of the more critical key risk

[10] George Westerman and Richard Hunter – IT Risk: Turning Business Threats into Competitive Advantage.

indicators that financial institutions can use to assess certain aspects of cyber risk within the organization.

Capital for Cyber Risk

Operational risk capital is increasingly becoming an important aspect of capital adequacy. The risk managers need to make sure that a financial institution holds enough capital for unexpected losses that might arise from banks' information technology and cyber risk management processes. The important thing to consider here is that capital for cyber risk should be held for those events that are generally rare, but can have a significant impact either on the bank or the whole financial system. As a result, operational risk capital should include events that arise from information technology risk.

Information Technology Risk Management

Considering the fact that information technology risk is one of the main areas of operational risk, which also includes cyber risk, it is vital for risk managers to cover all important aspects of information technology risk, including cyber risk.

In addition, risk managers should concentrate both on the so-called idiosyncratic IT risk, that is specific to an individual financial institution, as well as systemic IT risk. Systemic information technology risk might stem from the use of a single technology, such as a core-banking system by multiple financial institutions, or it could potentially also come from the dependence of the financial system on the telecommunications sector, where the inability of the telecommunications provider to reliably provide Internet or other networking services, can have an adverse effect on the financial system.

Causal factors of information technology risk

Despite the widely held view that information technology risk is caused either by a failure in technology itself, or by employees working at the operational level of the organization, information technology risk is often the result of a lack, or failure in the control function at the executive level of the organization. This stems directly from inadequate management of information technology at the top levels of the organization.

The abovementioned failure in control leads to weak, ineffective or inadequate chain of decisions which in turn leads to inadequate business processes, the result of which is ineffective risk, uncontrolled complexity and inattention to risk. As a result, it is the job of the risk manager to assess financial institutions in terms of this risk, which can have adverse implications for the financial institution.

IT risk management is built on three core principles, which the risk managers should closely supervise and assess[11]. These include:

1. Well-structured Foundation of IT assets
2. Well-designed and executed risk governance process
3. Risk-aware culture in which everyone has appropriate knowledge of risk and in which open, nonthreatening discussions of risk are the norm.

Well-structured IT foundation consists of technology that is not complex, including the information systems that are being used by the organization. In other words, the technology that is being used by the financial institution is only as complex as needed. In addition, a well-rounded IT foundation also consists of standardized infrastructure and consistent process definitions that are formalized (documented).

The risk managers also need to assess that a financial institution has a good IT risk governance in place. This should be the kind of process where organization has, and incorporates an enterprise-wide, holistic view to managing IT risks within the organization. The risk management process should clear and understandable, allowing the financial institution's lower-level managers to independently make decisions about IT in an informed manner.

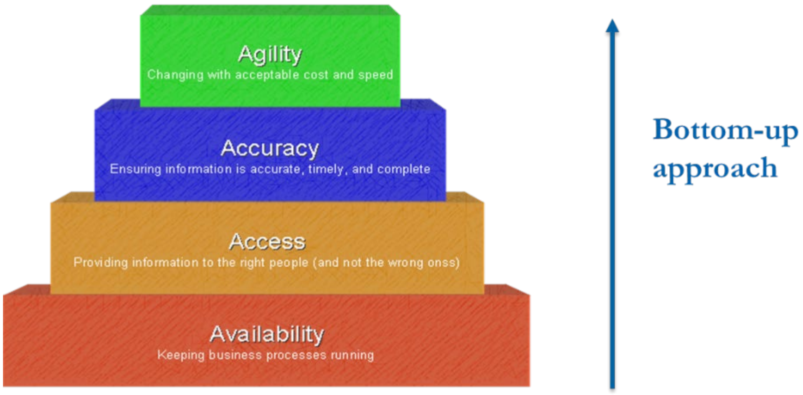
[11] Ibid.

Last, but not least, the most effective preventive control for dealing with IT risk, including cyber risk is a risk-aware culture. The risk managers should aid and support financial institutions in their process of improving awareness about information technology risk within their organizations. The financial regulators, on the other hand, should check and assess the level of awareness within banks and other financial institutions, in order to gain an understanding of how well-informed an organization's employees (including top management) are in terms of information technology risk.

Information technology risk supervision using the 4a framework

Risk managers should take a comprehensive approach towards IT risk supervision in the financial system. The approach should be based on addressing availability, access, accuracy and agility risks of financial institutions, including banks. This is a bottom-up approach towards risk management, which assumes that availability (risk) is at the bottom of a four-step pyramid, without which access, accuracy and agility risk cannot be mitigated. Likewise, accuracy and agility risk depend on availability and access risk, while agility risk depends on availability, access and accuracy risk, which precede it. The aforementioned model is also called the 4A framework for managing IT risk, since the four key areas of IT risk that are covered in the model include availability, access, accuracy and agility risk. Figure 3 shows the 4A approach towards IT risk management, involving the 4-step pyramid.

Figure 1. 4A IT Risk Management Model


Agility
Changing with acceptable cost and speed
Accuracy
Ensuring information is accurate, timely, and complete
Access
Providing information to the right people (and not the wrong onss)
Availability
Keeping business processes running
Bottom-up approach

Source: Westerman & Hunter

Availability risk consists of all potential scenarios that pose a risk to the organization's information systems and associated processes that are linked to systems and processes becoming unavailable or inaccessible. Availability risk is closely linked to an organization's business continuity management processes. It must be mentioned that availability risk increases when a financial institution such as a bank uses many different information systems that are not standardized.

Access risk comes from insufficient or inadequate access controls to an organization's information systems. Access risk can arise from insufficient internal controls. This can include such topics as network segmentation that is not implemented properly or unreliable network services, among others.

Accuracy risk is the risk that is associated with the storage, use and processing of data and information that might be stored in an organization's information systems. A major contributor to accuracy risk is a lack of a single data exchange standard for information systems, the result of which can lead to the manual transfer and conversion of data that is stored in different systems. Accuracy risk also increases with the complexity of information systems that are being used by a financial institution.

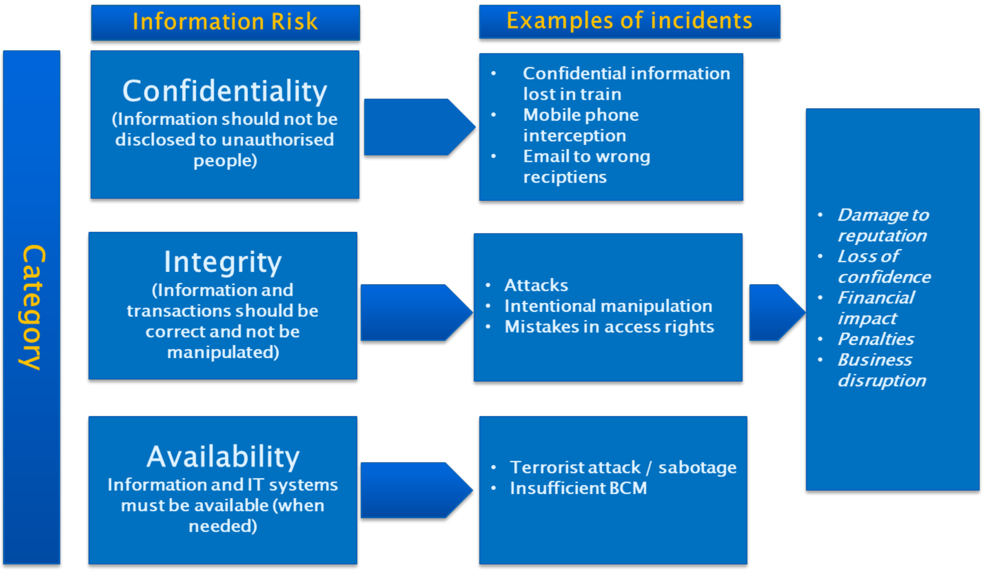
Agility risk can be caused by inflexible processes and systems that are difficult to either merge or separate. Poor project management practices as well as bad communication and coordination between an organization's business units and information technology employees/structural units can lead to increased agility risk.

Information Security Management

Information technology risk supervision should include cybersecurity/information security. The 4A framework's access risk component covers many aspects of cyber and information security. In addition, the other steps of availability, accuracy and agility risks also address cybersecurity and information indirectly.

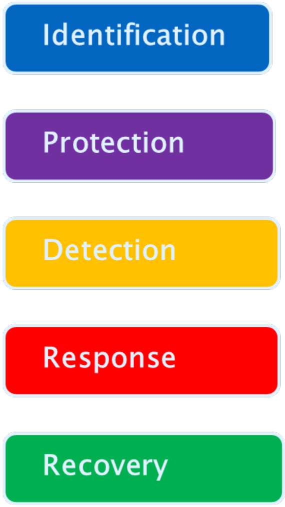
On the other hand, the financial regulator should also adopt a specific cybersecurity framework or standard that has been reviewed and is based on a globally accepted approach (i.e. NIST or ISO). Figure 4 provides a description of information security management and its subcategories of confidentiality, integrity and availability, based on the ISO information security management standard.

Figure 2. Information security management


Information Risk
Examples of incidents
Category
Confidentiality
(Information should not be disclosed to unauthorised people)
Confidential information lost in train
Mobile phone interception
Email to wrong recipitiens
Integrity
(Information and transactions should be correct and not be manipulated)
Attacks
Intentional manipulation
Mistakes in access rights
Availability
Information and IT systems must be available (when needed)
Terrorist attack / sabotage
Insufficient BCM
Damage to reputation
Loss of confidence
Financial impact
Penalties
Business disruption

A commonly used framework to assess contemporary cyber risk within the financial system is a model based on the NIST framework. The NIST framework is an easily adaptable methodology that incorporates five separate functions that need to be addressed from a cyber risk perspective. This includes identification, protection, detection, response and recovery processes associated with a financial institution's information assets and systems.

Figure 3.Cybsersecurity Management using the NIST Framework



The five functions mentioned above, cover most, if not all aspects of cyber risk that might arise within a financial institution. This includes the identification of all key information assets that an organization has and the methods that are needed to protect these critical assets. Additionally, the NIST framework outlines the detection processes and the relevant detective controls that need to be in place, in order for an organization to detect anomalous activity within its information systems. Last, but not least, the framework covers incident response and business continuity in the form of recovery processes, which is a key aspect of cyber resilience.

Information Systems Audit and Penetration Testing

Considering the increased dependence on information technology and the level of adoption of information systems, financial institutions should conduct both independent information systems audits and penetration tests. By the term independent, it is meant these organizations must conduct either internal, or external independent audits or penetration tests. This is important because the conduct of financial audit, which often covers IT general controls, is generally not enough to cover all important areas of the organizations' information systems environment. As a result, and at a minimum, the information systems audit should cover cybersecurity and those aspects of business continuity that deal with information systems.

Penetration tests are also vital to the effective and secure functioning of modern financial institutions. According to Michel, "penetration (pen) tests are critical to operating and maintaining an effective information security program."[12] It can be said that penetration tests are a form of an operational stress test, the aim of which is to reveal potential vulnerabilities and weaknesses an organization's information systems. In addition, one of the key benefits of conducting penetration tests is to raise the level of awareness within financial institutions, including at the executive level, about the importance of information/cyber security. Many financial regulators have requirements for penetration testing, but it is important to mention that this process does not cover the simulation of distributed denial-of-service (DDoS) attacks or other actions, which can potentially harm a financial institution or its clients.

Outsourcing

Outsourcing is defined as the use of a third party (either an affiliated entity within a corporate group or an entity that is external to the corporate group) to perform activities on a continuing basis that would normally be undertaken by the regulated entity. Financial institutions can outsource different activities, but the most common activities being outsourced are information technology and financial administration. Reasons for outsourcing differ, but according to the European Central Bank that carried out a survey in 2004, the two main reasons are cost reduction and access to new technology. Outsourcing also includes cloud computing and the organization should address outsourcing risk that stems from

[12] Michel, B. (April 17, 2017). The Validity of Penetration Tests. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/the-validity-of-penetration-tests.

cloud computing, since many financial institutions have begun to use the cloud for the provision of various financial services.

From a risk management perspective, any outsourcing agreement that deals with the provision of financial services, or associated technology/information systems, should be conducted in a manner so as not to hinder the ability of risk managers/regulators to reconstruct the activities of the organization in a timely manner, if necessary.

In addition, risk practitioners should also address the use of foreign service providers within the context of outsourcing. For examples, issues such as a financial institution's use of a foreign-based third-party service provider and the location of critical data and processes outside of the home country must not compromise the risk managers' ability to examine the bank's operations. As a result, risk managers should make sure that the outsourcing relationship is conducted in a way that does not diminish the risk managers' access to data or information needed to supervise the financial institution. Outsourcing to jurisdictions where full and complete access to information may be impeded by legal or administrative restrictions on information flows should not be acceptable to the risk manager.

Risk practitioners should also check that financial institutions conduct adequate risk assessments regarding the planned outsourcing arrangement, which can include a comprehensive analysis of any, and all available information about the service provider (company) which is accessible to the bank. The risk assessment must, at a minimum, include a thorough review of the latest (most recent) independent financial/information systems audit report, if such document/s exists[13]. If required, and based on the request from the financial regulator, the financial institution such as a bank must submit the risk assessment, along with the

[13] Regulation of the National Bank of Georgia on Operational Risk Management within commercial banks.

service provider’s audit report to the financial regulator. Annex 3 offer s a checklist for the assessment of outsourcing risk.

Other topics that need to be considered in this respect include requirements for business continuity management. The financial institutions’ business continuity plan must include provisions to ensure timely access to critical information and service resumption in the event of unexpected national or geographic restrictions or disruptions affecting a foreign service provider's ability to provide services.

It is worth noting that not all outsourced activities of a bank can pose all or some of the risks mentioned above. Therefore, a concept of materiality plays a significant role here. An outsourced activity is material if its disruption could potentially have a significant impact on the bank’s business operations or its ability to manage risks effectively. Some factors that could help in considering the materiality of the outsourced activity are provided below:

1) The financial, reputational and operational impact on a bank in case of the failure of a service provider to adequately perform the activity;
2) Potential losses to a bank's customers and their counterparts in the event of a service provider failure;
3) Consequences of outsourcing the activity on the ability and capacity of a financial institution to conform with regulatory requirements and changes in requirements;
4) Cost;
5) Interrelationship of the outsourced activity with other activities within the bank;
6) Affiliation or other relationship between the financial institution and the service provider;
7) Degree of difficulty and time required to select an alternative service provider or to bring the business activity in-house, if necessary;

8) Complexity of the outsourcing arrangement. For example, the ability to control the risks where more than one service provider collaborates to deliver an outsourcing solution.

Material outsourced activities often include various information technology functions supporting a bank's core businesses, business continuity management (BCM) arrangements and business recovery facilities, claims processing, marketing and research, etc. In some cases, financial institutions may also outsource their information security function to an outside organization or entity. Non-material outsourced activities are typically (but not always) those where there are numerous service providers in the marketplace, the agreement is short-term (e.g. less than 12 months), the cost of switching between providers is low and switching is relatively easy (e.g. utility, printing services, etc.).

An underlying principle of outsourcing bank activities is that a bank's Board and senior management retain overall responsibility for their outsourcing policy and all outsourced activities undertaken under that policy. In other words, the use of service providers does not mean that the financial institution is not responsible for outsourced activities. The organization's management must make sure that outsourcing is conducted in a safe and sound manner and in compliance with applicable laws and regulations. The role of the internal audit is important in this regard.

Crisis Simulation Exercises

Since cyber risk is a systemic operational risk, it makes sense to conduct cyber exercises to test the readiness of financial system participants. This is a form of a stress test that is often associated with either information technology or operational risk.

In order to gain a maximum benefit from crisis simulation exercises, multiple organizations and entities can be involved in the implementation of crisis simulation exercises. These might include commercial banks, the Ministry of Finance, CERT, internet providers, and others.

General Topics for Consideration when Assessing Information Technology Risk

Causes of IT Failures

The probability of an event associated with an IT failure is due to four main factors. These are:

1. Complexity (of information systems).
2. Change (associated with information systems and related processes).
3. Vulnerability to various information technology **threats, including cyber-threats**
4. Maturity of the information (IT) systems that an organization uses

The impact and potential damage associated with an IT failure is mostly determined by how material an IT failure is to an institution (for example, can a bank easily switch to manual processing for all of its critical services).

A financial institution's statistics, such as system downtime and outage reports, root cause analysis, security incident reports and fraud loss data can be a good instrument for identifying and assessing inherent risk that is associated with information technology.

When trying to determine the inherent risks within the IT environment, risk managers should look at the following categories/topics:

Complexity of IT systems

As a rule of thumb, the greater the complexity of an organization's information systems, the more likely it is that problems may happen. The complexity of information systems is determined by the number of information systems used by an institution and the level/degree of sophistication of interrelated applications and infrastructure components. When assessing information systems complexity, risk managers should closely look at the level of diversity in financial products, physical locations and outsourcing service providers of the financial institution.

In most cases, an organization's list of information systems, infrastructure (network) and application architecture documentation can provide the basic information required to assess the complexity of the IT systems environment.

Change within the IT systems environment

Risk managers have to assume that change often leads to an element of uncertainty into systems. Changes can happen due to new business requests, normal maintenance activities or problem resolution associated with information systems. The level of risk that comes from system changes is directly related to the materiality/significance of the change to the original system. In addition, the risk can also come from people that are unable to properly assess whether the change in one system can have unwanted effects on other systems or processes. This applies to both changes in IT programs and applications as well as IT infrastructure.

A risk manager should check an organization's IT project portfolio and IT change register, which can offer information that is required to assess the level of change that is present across the IT systems environment of an institution.

Vulnerability of IT systems to internal and external threats

Vulnerability, from a risk management perspective, measures the level of exposure that the information (IT) systems have to threats, both internal and external to the organization. Overall, IT systems that can be exploited maliciously for personal interests (financial or non-financial) will be subject to more threats. IT Systems that allow access to cash or other monetary reward are usually targeted (for example, Pawn shop/Lombard loan systems, ATM, Internet Banking and other systems).

If a threat is able to effectively exploit a vulnerability, the institution has the risk that its IT systems will be compromised/hacked. An institution's fraud and security incident history (both internal and external), and IT risk register are useful in assessing the IT system's vulnerability.

Maturity of IT systems

Institutions with IT systems (including technologies) that have a proven track record of functioning well with minimum system failures and disruptions over time, may experience fewer problems than those with IT systems that are new. In the case of new systems, there might be problems or issues, that are not as well understood.

Risk managers should also take into consideration that more mature IT systems may be legacy systems, which are difficult to update since there may be few people who can support the system, or who understand the system.

An institution's IT strategy and the age of key systems can be useful in assessing the maturity of its IT systems.

One significant aspect to consider when assessing an organization's cyer risk is the complexity of its information (IT) systems. From a general perspective, an information system consists of applications, hardware, databases, networks and people. Complex information systems are not necessarily characterized by high levels of cyber risk, if they are managed adequately by the organization. On the other hand, poorly managed information systems that are also complex in nature can be prone to increased cyber risk. Some fairly common examples of information systems complexity include a large number of connected, or interrelated systems. It is worth noting that even a large number of independent systems may pose a considerable challenge to financial institutions. In addition, unused (or largely unused) information systems that have not been removed, but allow access to various employees can pose a considerable threat. The latter can also pose the threat of fraud to the organization, since unauthorized modification of data might also take place in such systems, which can be linked to financial fraud events.

When evaluating the complexity of information systems, other factors can also be taken into consideration. For example, a high number of problems stemming from system changes, as well as duplication of data are often the end-result of complex information systems, since data may be questionable when several different databases are used to store the same or similar data.

Business Disruption

There are certain events, which can happen, that might be beyond the control of a bank/institution. In some cases, a material, or severe event may result in the inability of the institution to fulfil some or all of its business obligations, particularly where the physical, telecommunication, or information technology infrastructures have been damaged or made inaccessible. In the case of a cyber-attack, the network can be brought down for fairly long periods of time, making it very difficult for a financial institution to offer its critical services such as online and mobile banking as well as other processes to its clients. This can, in turn, result in significant financial losses to the institution, as well as broader disruptions to the financial system through various channels.

Risk managers need to review and determine the potential sources of risk that can lead to system disruptions and business failure. For example, the risk managers should look at whether there are any specific business disruption scenarios which the institution is particularly vulnerable to such as a small bank whose business activities are concentrated at a single location. For a larger institution, business disruption risk may come from the close proximity of the primary data center, or server room to the secondary data center or server room. This can happen, when for example, both the primary and secondary server rooms are located next to each other. The business disruption risks are generally related to the infrastructure (IT and building) and staff (pandemic). Risk managers should consider that where the location of the head office is in a riskier place, such as next to a government building, or places that are prone to additional risks, then the institution should have plans around possible physical disruption to its opertaions and access to the building.

Security management

The supervised institution should make sure that there are adequate policies and procedures in place to protect its information assets from internal and external threats to confidentiality, integrity and availability. This category also includes cyber risk. Cyber risk should be included within the wider context of information security.

When assessing security management, risk managers should look at:

Approved Policies and Standards – **It is generally not enough to have an information security policy and procedure that is in draft form and has not been approved. Unapproved policies and procedures are often not followed.** An institution should have an IT security policy framework which consists of a set of effective policies and standards. The institutional policies should be approved by executive management, and should be available and communicated to all employees. The policies should include the rights and responsibilities of all employees for security. Employees should be required to read and sign the relevant policies to indicate their understanding.

Prevention - **The most effective preventive control is the level of awareness of an organization's employees. The risk managers should therefore check a wide array of preventive controls and whether they work within the institution. This also includes employee awareness about information security and cyber risk.** Institutions should have processes and systems in place to prevent unauthorized access to, or software execution on, the internal network(s). Typically this includes such components as firewalls, logical access controls, anti-virus software, intrusion detection and other components.

Monitoring – Organizations need to have relevant detective controls to identify potential unauthorized activity within its information systems environment. Risk managers should check to make sure that the relevant detective controls are in place and are effective. Institutions should have processes in place to monitor ongoing security risks and detection/response to security incidents in a timely manner.

Testing - Controls should be subject to independent testing to assess that the controls in place to mitigate security risks are adequate and being followed. Testing may be provided by Internal and External Audit, as well as the use of specialist, independent contractors hired to assess the security environment. Institutions operating web-based transactional systems must have penetration testing performed by an independent third-party at least annually.

Track Record in IT Security – In order to assess the adequacy of an institution's security policies and procedures it is useful to gain an understanding of how successfully the organization has detected security breaches in the past. It is important for risk managers to ask what security incidents have occurred within the institution and how they were mitigated (addressed).

Application development and maintenance management

Risk managers should check to make sure that financial institutions have a strong control framework for developing and maintaining computer applications. Lack of controls in this area can result in instability of systems, undesirable or erroneous system changes or the inability of computer applications to support the objectives of the business.

When risk managers assess application development and maintenance, risk managers should consider:

System changes – Any planned or ongoing changes that are made to the system should be reviewed, authorized and controlled.

Methodology – There should be a formal methodology that provides a consistent framework for application development and maintenance.

Governance and Monitoring – There should be a uniform framework for managing the institution's set of applications. The framework should be in place for ensuring that business objectives are accomplished.

Development and Testing – Any changes to programs/applications must be conducted in a separate environment from the production environment. User acceptance testing that is followed by formal signoff from the business should be conducted before programs are put into production. It is recommended that testing environments should be similar to the production environment, in order to reduce the risk of changes in application behavior when deployed to the production environment.

Source Control – Risk managers should check to see that strong application source code controls are implemented by the institution.

Application Documentation – There must be appropriate documentation that covers how a program, or an application works. The documentation should be maintained as part of the application development and maintenance process. At the very least, there should be a complete register of programs/applications that an institution uses, which identifies the people responsible for conducting development and maintenance activities on each application, the nature of the application and the technology employed.

Previous History with Application Development and Maintenance – Risk managers need to assess how successful a financial institution has been with previous application development projects as well as with the maintenance of information systems. Post Implementation Reviews and the number of failed application deployments are good indicators of this. A review of the list of user requests (completed and pending) will also provide an indication of the extent and rate at which business needs are being addressed.

Good Practice

- Risk managers should check to make sure that formal processes are implemented for authorizing, administering and regularly reviewing user access to the network, applications and remote access. As a general rule, developers should not have access to the production environment.
- The use of a vigorous penetration testing strategy that requires all network layers to be tested is considered good practice. It must be mentioned that at least some of the financial institutions incorrectly assume that their organization is secure just by testing the network perimeter of the organization. The penetration testing process should cover the security of the other defensive layers (e.g. web application, database).
- Code review by peers, if possible, should also be conducted to ensure that an appropriate level of quality, consistent, maintainable code is being delivered. Ideally, there should be a formalized review processes and coding standards to ensure quality deliverables.
- It is recommended that risk managers also check whether agreed application development standards, including interface and technology standards and an exemption procedure are in place.

Business Continuity Management

Business Continuity Management (BCM) is a critical component of an institution's risk management framework, ensuring that the organization is able to meet financial and service obligations to clients and other stakeholders. Institutions may face significant losses or even fail as a result of not being able to recover from business disruptions and restore critical business operations in a timely manner.

BCM should be a process that covers the whole organization, or even the holding group of a financial institution and just a few structural units (i.e. divisions or departments) or certain aspects of the institution[14].

Institutions must consider different types of possible scenarios to which the financial institution may be vulnerable. These scenarios might include natural disasters such as floods, earthquakes and fire, as well as man-made events such as cyber-attacks.   Annex 4 provides a business continuity checklist for assessing the quality of business continuity management within financial institutions.

Board approved policy

An institution should have a policy which sets out its approach to business continuity management. Ideally, there should be a business continuity policy within the organization. This must be approved by the Board of Directors.

BCM components

BCM is a term that is used to cover several different underlying components (i.e. Business Impact Analysis, Risk Assessment, Recovery Strategy, Business Continuity Plan, Disaster Recovery Plan (IT Recovery)) and the regular review, testing and maintenance of these components.

[14] Papuashvili, D. (2013). Effective Business Continuity Management. Journal "Economics and Banking" (Georgian). Volume 2. Tbilisi, Georgia.

- **Business Impact Analysis (BIA)** - The BIA is a process that is used to define critical business functions or processes of an organization, including resources and infrastructure of the institution and the maximum downtimes for these before a disruption has a material impact on the institution's operation. Critical business functions/processes of a financial institution might include its core banking processes, online and mobile banking, its real-time gross settlement system, as well as communication systems such as electronic mail (e-mail).

  The BIA should involve active participation by senior management and ensure an adequate representation from all potentially impacted business functions.

  When conducting the business impact analysis (BIA), the institution needs to assess the probability of a financial or a reputational loss for each function/process within the institution[15]. The probability of such a financial or reputational loss should be weighed against the impact of a significant disruption for each business process. The BIA should include:

  - Evaluating the impact of a disruption to business operations in the event of a loss of a critical business process for defined periods of time. The probability of such an event should also be determined;
  - determining alternative sources of information/services available;
  - establishing the financial or reputation cost of business disruption and the probable recovery time for each critical business; and
  - identifying specific threats to the critical business processes, including assessing the geographic location of data centers, branches and other aspects of an institution's operations..
- **Risk assessment** – The financial institution needs to conduct a risk assessment, that also includes risk analysis. A Risk Assessment (which is sometimes done as a part of the BIA) should be undertaken to identify the potential disruption

[15] Ibid.

scenarios that may disrupt the critical business functions, resources and infrastructure. Such scenarios might include floods, earthquakes, fire, war, cyber-attacks, etc.

- **Recovery strategy** - Based on the outcome of the BIA and Risk Assessment, the institution's Recovery Strategy should be devised and implemented. This may involve the use of an alternate operational site or a data center. A key risk to be mitigated when using an alternate operational site is that the primary operational site and alternate operational site are not unavailable simultaneously due to close physical proximity and/or shared critical infrastructure such as power and telecommunication networks.

  Consideration should be given when establishing appropriate off-site storage that arrangements are made for critical data and specialist software, covering frequency of updates, remoteness from the prime site, processing capability, responsibility for back-ups and the maintenance of adequate documentation on how to use the back-ups.

Business Continuity Plan (BCP)

The business continuity plan consists of a set of documented instructions, procedures and information which enable the institution to:

- respond to a material disruption to normal business operations;
- recover and resume critical business functions; and
- plan to return business to normal operations.

While the BCP is a corrective control mechanism that needs to take into consideration the specific requirements of the institution, at a minimum the BCP must include:

- the procedures to be followed in response to a material disruption to normal business operations;

- a list of all resources needed to run operations in the event the primary operational site is unavailable;
- a communication plan for notifying key internal and external stakeholders if the institution’s BCP is invoked;
- consideration of business continuity as part of any material outsourcing agreement with a critical third- party service provider; and
- relevant information about an institution’s alternate site for the recovery of business and/or IT operations if this forms part of the institution’s BCP.

Off-site copies of the BCP must be kept by a number of responsible managers who have designated responsibilities in terms of the BCP and should also be available at the alternate recovery site if applicable.

In assessing the BCP, risk managers should consider aspects of the BCP, including the testing program and ensuring this is updated.

In addition, the BCP team must have updated contact information of all BCP team members and other relevant people both within the organization and outside of the organization[16]. The contact information can be listed on a special contact card that the BCP team members can easily fit in their wallet or purse.

Disaster Recovery Plan (DRP) for IT recovery

The DRP is the information technology component of the institution’s business continuity plan (BCP) and covers the documented procedures, instructions and information which allow the institution to:

- respond to a material disruption to critical IT systems;
- recover and restore critical IT systems in an orderly manner; and
- plan to return IT systems to normal operations.

[16] Ibid.

Recovery priority and timeframes included in the DRP need to be agreed with the business and must be consistent with the contents of the BCP.

While the DRP should reflect the specific requirements of the institution, at a minimum it should contain:

- the procedures to be followed in response to a material disruption to critical IT systems;
- recovery priorities and timeframes, as agreed with the businesses;
- a list of all resources needed to run IT operations in the event the primary operational site is unavailable;
- a communication plan for notifying key internal and external stakeholders if the institution's DRP is invoked;
- consideration of IT recovery as part of any material outsourcing agreement with a critical third-party service provider; and
- relevant information about an institution's alternate site for the recovery of business and/or IT operations if this forms part of the institution's DRP.

Review, maintenance and testing of BCM

The BCM components must be reviewed regularly (for example, at least annually). In addition, the BCP also needs to be tested at least annually. Furthermore, maintenance procedures associated with business continuity management also needs to be done regularly. This is done to make sure that any changes in either the business continuity risk profile and/or operations are captured.

Testing is an important component of business continuity management, since it validates the procedures included in the BCP and DRP to make sure that they are able to meet the institution's business continuity objectives.

Outsourced business functions

Service providers should have adequate business continuity arrangements in place and this should form part of the 'due diligence' process undertaken by institutions when considering entering into an outsourcing arrangement.

The institution needs to have a documented and approved outsourcing policy that also covers cloud computing. This is due to the fact that an increasing number of financial institutions are beginning to use the cloud for the provision of financial services, as well as information technology-related processes for their everyday operations.

The ongoing maintenance of the service provider's business continuity arrangements should be regularly monitored by the institution. The risk managers should check whether this is done by the financial institution. This is particularly important where there is no capacity to bring the outsourced function back in-house. As a result, the risk managers need to check whether the institution has sufficient knowledge of certain functions that might be brought back into the organization. These are processes that have been outsourced. Additionally, the risk managers might want to check to see if the institution retains sufficient internal knowledge and experience for the provision of critical financial services such as core banking and other related functions.

Good Practice

The components of a business continuity plan should be regularly reviewed, tested and maintained. At some larger institutions these components should be reviewed more frequently than annually.

A strategy that provides for continuous availability of the identified critical business functions is considered good practice, however the use of such a strategy is for the institution to determine having regard to the risks and costs involved.

Potential impacts on business continuity arising from new major project initiatives should be considered at the project planning stage.

Where shared alternate operational sites are used in recovery good practice is to contract for dedicated (i.e. guaranteed) recovery space rather than relying on availability of shared (i.e. non-guaranteed) space. At a minimum, it is important that institutions understand the order of priority they would have to the facilities should multiple clients be entitled to use the facilities at the same time.

Better practice BCP and DRP documentation is clearly structured and sufficiently comprehensive so that staff can quickly locate the component relevant to them and enact their role, without needing to make decisions in a crisis situation. Separation of the recovery documentation from the recovery strategy can aid in the interpretation of the documentation.

Potential Risk Areas for Consideration

One of the key problems associated with business continuity management is a lack of comprehensive testing. Quite a few organizations either test the business continuity plan only partially, or they do not test the business continuity plan as frequently as they should. An important deficiency in this respect is the fact that many organizations tend to focus excessively on information technology recovery and focus less on people and their safety. In addition, the ability of people to recover from large operational events or incidents should be the top priority of the organization.

In addition, employees of an organization may need additional training, since they might not have received enough training. This includes the identification and proper clarification of responsibilities, improved reporting to the Board of Directors and senior management, as well more testing of the plans itself.

Other problem areas include the fact many business continuity plans can be out-of-date and might not have been renewed. As mentioned earlier, important components of the BCP might not be tested. This applies to areas such as the evacuation and DR plans as well, where the plans are insufficiently tested and do not cover the right/necessary offices of the institution, or do not cover key systems during the recovery process.

Another key aspect to consider is whether the BCP addresses unexpected events and risks that the institution might face. Often, insufficient attention is paid to unexpected events that can have significant effects on the institution.

Potential Areas of Concern for Other Key Topics

Infrastructure

There are a number of factors that should be assessed for potential problems under the financial organization's infrastructure. For example, improvised, informal and ad-hoc security policies that have, or have not been approved and that were developed in response to a new security weakness that are not integrated into a comprehensive security framework can increase an organization's overall risk profile. The use of generic security polices, not tailored to address the particular risks of the institution should also be avoided. In addition, if some of the policies are out of date, unsigned, unapproved, in some cases unauthorized, and incomplete or, in draft form will likely increase the risk that an organization faces.

Unfortunately, quite often there is also lack of a formal, documented process to grant security exemptions or a central registry to record those that have been granted exemptions does not exist. In some cases, there is an insufficient, or a failed patching process that can significantly impact a financial institution. Viruses that are sent via email, for example, can get into an institution's network and infect unpatched systems and cause significant damage are require cleanup by the organization. If the organization does not conduct independent external penetration tests that cover the financial institution's network-connected systems can also increase the overall risk exposure.

Security

There are also a number of areas of concern when reviewing the security practices of the organization. This may include both cyber risk as well as risks stemming from an inadequate physical security management process. Fairly frequently, access controls within financial institutions are out of date and are not reviewed regularly by business owners. It must also be mentioned that if the IT of the institution does not provide timely access reports to business owners, this can also be a source of operational risk.

From the point of view of password management, weak password policies, or a lack of a password policy can serve as a risk indicator to the organization. If there are short, easily guessable passwords or dictionary words being used as passwords by the organization, this can directly increase cyber risk (and the risk of fraud). Some of the other factors to look out for include:

- Accessing systems by multiple people that use the same username and password. Company employees sharing of passwords to allow multiple users to access the same system account.
- Programmers/developers have access to production systems.
- Patches are not applied in a timely manner.
- The asset (referring to information assets) register is out of date.
- Service levels are not defined and/or formally agreed with businesses.

When it comes to physical security, it can be generally assumed that physical security and cybersecurity often go hand in hand and that physical security is often the underlying foundation for an organization's operational risk management framework. Without physical security, cybersecurity can be impossible to manage. This is because physical security can affect cybersecurity directly. For example, if an unauthorized individual breaks into a bank's server room and damages the server that hosts the organization's core-banking system, it may be difficult to recover from such an event in a timely manner[17].

Application development and maintenance

Application development and maintenance are critical components of the overall cyber risk management framework. To offer an example, an insufficient impact analysis of a change that results in a failed change can have a potentially large impact on a financial institution. Furthermore, poor quality business requirements or lack of business involvement/signoff in application changes resulting in an application which does not meet the business needs can be a considerable source of risk to the organization. For larger institutions, the absence of an overarching set of standards or design (architecture) leads to an increase in the overall complexity of the application environment resulting in an increase in development and maintenance costs. The loss of corporate knowledge (e.g. due to redundancies, resignations, poor documentation) can also negatively impact the financial institution. If the organization does not know how to perform some of its critical processes that it used perform with relative ease earlier, this is something to be addressed (and mitigated) as early as possible. The widespread use of user-developed applications such as Excel spreadsheets, Access databases and other programs which are not subject to appropriate application development controls can also significantly increase the level of cyber risk within the organization.

Project Management

All financial institutions have projects of various forms and sizes. The success and competitive advantage of organizations often depends on effective and efficient project management. Therefore, it is important that institutions have a strong control procedure for project management. Project outcomes (e.g. major process / systems change) may introduce risks if not fully considered.

[17] The recovery process largely depends on the business continuity measures that an organization has in place, but oftentimes it is challenging for organizations to recover from physical incidents in a timely manner, even with fairly comprehensive business continuity processes.

Methodology

A formal methodology provides a good foundation for the implementation of various projects. It is important that institutions conduct a risk assessment as part of significant project initiatives (i.e. before project implementation).

For example, a major (core) system project should follow an established method such as Systems Development Life Cycle (SDLC). This includes determination of the business requirements (i.e. business case), functionality requirements, the development of the system, user acceptance testing, implementation and Post Implementation Review.

Governance and Monitoring Arrangements

From the perspective of project management, there should be a formal methodology for implementing projects. There should be a clear governance structure for project management. There should also be clear roles and responsibilities for the project, as a whole.

It is recommended that the institution have a formal project schedule for the tasks that need to be achieved and for the activities that need to be carried out for the scope of the project. The institution should also have a monitoring process for tracking the progress of the project. Additionally, there should also be reporting that includes issue escalation and resolution, as well as other similar topics. **Risk managers should check to make sure that such processes exist within the institution.**

History of Project Management

When an institution decides that it wants to start a major new project, it is useful to analyze the kinds of projects that have been implemented/carried out in the past and whether the process was successful. Another important aspect to look at is if the institution analyzed what it did right and what it potentially did wrong with the previous projects. Risk managers should look at these topics, since in certain instances, financial institutions seem to show that they have been successful at managing various projects, while in reality the process has not been very effective. An indicator to look at in this area is whether project managers have been replaced or changed often during the course of the project, or if there are significant delays in how the project is executed.

Good Practice

A project management methodology that clearly outlines the overall project management framework adds a control to the process and mitigates the risk of (poor) decisions being made by individual business managers.

Risk managers can also check to see whether a project management office or a structural unit exists for managing project, especially the kinds of projects that are fairly large in size and cover multiple structural units within the organization.

The advantage of having a project management office, or a similar structural unit is that it provides a centralized specialist management control rather than simply adding the (same) responsibilities to a business manager who may be overloaded and/or not an expert in project management.

Internal audit

Internal audit coverage should be adequate to independently verify that the information technology risk management framework has been implemented as intended and is functioning effectively.

Internal audit should not simply be testing for compliance with board approved policies and procedures, but should also be evaluating whether the information technology risk management framework meets organizational needs and risk management expectations. For example, while internal audit should not be setting specific risk appetite or tolerance, it should review the robustness of the process of how these limits are set and why and how they are adjusted in response to changing circumstances.

Payment systems-related considerations

Risk managers should examine electronic banking and other forms of payment systems that a financial institution uses from the perspective of information technology risk, including cyber risk. These systems might include online (internet) and mobile banking as well as automated teller machines, point-of-sale (POS) terminals and other systems.

General topics that risk managers might want to cover when addressing electronic banking and other payments systems include:

1) Does the institution have adequate policies regarding the implementation, establishment and servicing of such systems?
2) Does the organization properly notify the risk manager when new products, processes and systems are introduced?
3) Are there relevant preventive, detective and corrective controls to ensure the safe and sound functioning of such systems?
4) Are there sufficient safeguards from tampering with payment systems terminals?

Does the institution perform information systems audit and penetration tests on the systems being used by the institution?

Risk Identification

Risk is an inseparable part of doing business. key component of the cyber risk management process consists of **risk identification**. It is therefore important for financial organizations, to have a robust and comprehensive risk identification process that addresses critical and relevant risks that the organization might face. Cyber risk identification is the first step in the risk management cycle[18]. The other components of risk management include risk assessment, risk response and mitigation and risk monitoring. According to ISACA, the organization's IT risk management framework, which closely aligns with cyber risk management, must be:

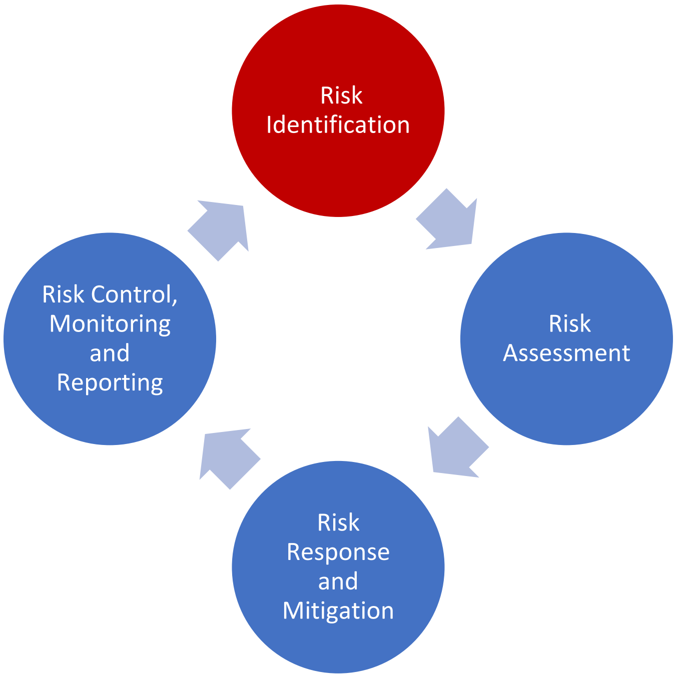
1. **Comprehensive** – The IT risk management process needs to be thorough and sufficiently detailed.
2. **Complete** – The process should be executed from beginning to end.
3. **Auditable** – The framework should be clear and understandable and be verifiable and validated by an independent third party.
4. **Justifiable** – The program must be based on valid reasoning and be commensurate with the size and complexity of the organization.
5. **Compliant** – The framework should be in line with relevant standards and potential legal requirements.
6. **Monitored** – There should be a regular review and supervision of the process
7. **Enforced** – The framework must be dependable, consistent and enforceable, as required.
8. **Up to date** – Must reflect the current environment of the organization, including processes, systems, people and external factors.
9. Adequately **Managed** – Sufficient resources must be allocated with relevant support from executive and senior management.

[18] ISACA

It cannot be stressed enough that cyber risk management should be integrated into the overall (enterprise) risk management process of the organization. Additionally, an important point to consider is that the IT management process within the organization must support the business and meet the relevant goals and objectives of the business, and not the other way around.

As has already been mentioned, risk identification is the first step in the cyber risk management life cycle. Without a thorough risk identification process, the overall risk management framework cannot and will not be effective. This is because only those risks that are properly identified and recognized can be acted upon and mitigated, as needed. If risks are not properly identified, or if the risk identification process skips or omits critical areas of the business (and organization in general), the risks will remain undetected and unconsidered (skipped) from the strategic planning process that should be carried out by senior management. As a result, unidentified risks can pose a significant and critical threat to the organization, especially when such risks can have a significant impact on the organization's operations. Figure 6 depicts the cyber risk management lifecycle, with cyber risk identification as its first step.

Figure 6. Cyber Risk Management Life Cycle

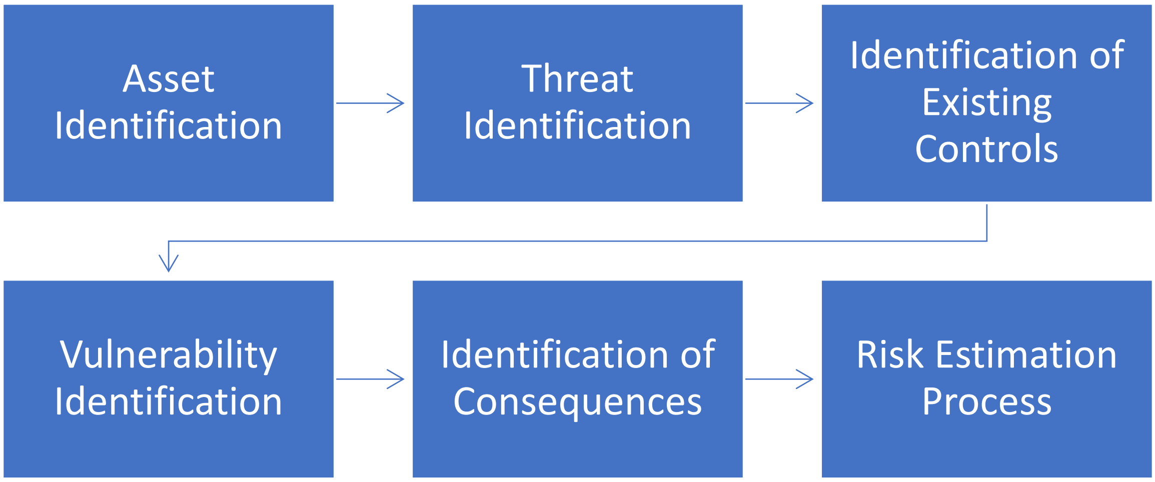

Risk Identification
Risk Assessment
Risk Response and Mitigation
Risk Control, Monitoring and Reporting

Source: ISACA

One of the best ways to diagnose how effectively an organization handles risk is by its risk culture. There are three main elements to an organization's risk culture. These include the organization's attitude towards risk-taking, attitude towards policy compliance and its behavior toward adverse outcomes, stemming from various events. When looking at the level of risk an organization is willing to take on, IT risk has to be considered. Furthermore, the organization's stance (including staff) towards following policies and procedures and policy adherence, in general, is crucial for effective risk management.

The process of risk identification itself consists of six general steps. These include the identification of assets, threats, existing controls, vulnerabilities and risk estimation. Figure 7 describes the risk identification process below.

Figure 7. Typical Risk Identification Process.


Asset Identification
Threat Identification
Identification of Existing Controls
Vulnerability Identification
Identification of Consequences
Risk Estimation Process

Source: ISACA

When identifying risks, the organization has several options to consider for the sources of risk. The organization may review its own historical operational losses to look for IT-related risk events. An internal operational risk report that contains information on the organization's information technology incidents can be used in this case. In addition, external loss events, such as those contained in an external loss database may also be used by risk managers. Other outside information such as threat intelligence from national CERTs, regulatory bulletins and similar sources may also be used.

The advantages of using Risk Scenarios

Incorporating risk scenarios into the risk management process allows an organization to enable communication and discussion on risk, which can stimulate and motivate people to take action about specific kinds of risk. Using risk scenarios also creates the kind of environment where the organizational staff can clearly understand what risks the organization faces. This, in turn, can help to establish the connection between business objectives and relevant cyber risks that might hamper the achievement of the business objectives.

Cyber Risk Scenario Development

A risk scenario may be defined as a description of a specific cyber-related risk event that can have an impact on business. The risk scenario typically comprises of the following aspects:

1. Threat - Potential for compromising security, or for creating an adverse impact on the organization.
2. Agent – Either the internal or external entity the is responsible for creating the threat.
3. Event – An operational risk event, such as a security incident or a systemic disruption the can be associated with the following:
    a. Theft or misappropriation of assets
    b. Unauthorized/unlawful modification of data, or information
    c. Inappropriate use of resources
    d. Changes to existing regulations that may have an impact on the organization.
    e. Lack of a change management process
4. Asset - An item of property, either tangible, or intangible (such as an information asset) owned by a person or company and regarded as having value.[19] Assets can be affected by a risk event. Assets can also be classified into the following categories:
    a. People
    b. Systems (both electronic and physical)
    c. IT processes
    d. Physical infrastructure
    e. IT infrastructure (including networks)

[19] Oxford Dictionary

    f. Data and information

5. Time – In many cases, the timing of a risk scenario can be relevant. This can include the aspects listed below:
    a. Duration (how long an identified risk scenario is expected to last)
    b. Timing (if applicable, when a specific risk scenario is most likely to occur)
    c. Detection (how can a specific event associated with a risk scenario be detected?)
    d. Time lag between the occurrence of an event and its impact on the organization

Risk Scenario Development Considerations

When developing risk scenarios, one of the first things to consider is that the organization and its processes change over time. As a result, risk scenarios will also likely change over time. In addition, in some cases, organizations can get carried away with the idea of risk scenario development and start developing a large number of potentially complex risk scenarios that are difficult to understand and manage. This should be avoided. One way to avoid this is to develop a standard set of generic scenarios at the beginning and then to transition to specific and more detailed scenarios for identified risks, as more details about the risk scenario become clearer to the organization.

Risk scenarios should be manageable and be realistic. They should also reflect the complexities and characteristics of the organization. For example, if an organization's data center is not affected by the risk of earthquakes, such a risk scenario should not be developed for the organization's data center. Conversely, if the bank's data center is located in a region that is prone to floods, then the risk scenario needs to be incorporated into the organization's risk management process.

Furthermore, it is very helpful, and at the same time important to develop a risk taxonomy for the risk scenarios. The organization can use a scale for rating both the likelihood and impact of risk events. These can be based on a numeric system that ranges from 1-5 in the order of importance, or use phrases such as "low", "medium" and "high." The scales that are used though, should be consistent throughout the organization and all structural units should use the same taxonomy (scale).

An additional aspect to consider are the skills and experience of people dealing with the development of risk scenarios. As already mentioned, risk scenarios should be relevant to the organization. Risk management should not develop the kind of risk scenarios that are unrealistic, or are not applicable to the operations of the organization. Therefore, the staff that is charged with developing risk scenarios should be knowledgeable and skilled. This means that risk managers must understand the nature and type of risk that the organization faces based on the existing (and potentially future) business processes.

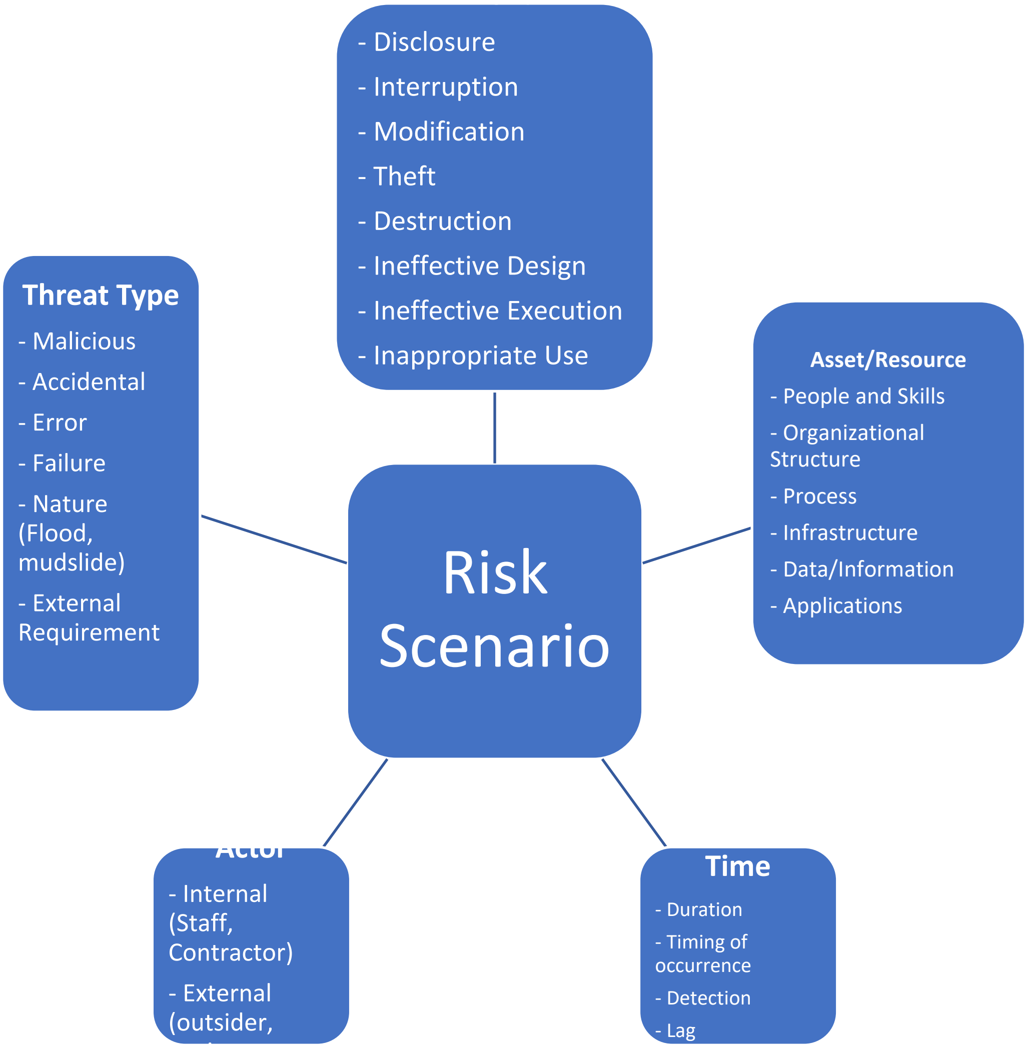
There should be a scenario building process within the organization that involves relevant stakeholders from other business/structural units outside of IT and risk management. Involving staff from other units and explaining the impact on business of the identified IT risks will aid the organization in gaining the support of both management and other stakeholders for allocating sufficient and adequate resources for IT risk identification and risk management, in general. It is important to stress and emphasize that the business unit from the first line of defense should be involved in the risk scenario development process. This is because the staff from the operational unit (first line of defense) have daily contact with the systems and processes that they manage and usually understand the vulnerabilities and existing IT risks in great detail.

An additional aspect to consider is not to focus too much on extreme and rare scenarios, where the likelihood of occurrence might be very low. From an operational risk management perspective, it is important to concentrate on both high frequency-low severity events as well as low frequency-high severity events, but if an event is very unlikely to occur, the organization should dedicate most of its resources to managing and identifying risks that are likely to occur.

Another point of consideration is to develop complex scenarios from the initial (less complex) risk scenarios that were developed by the organization. This is needed so that the important interconnections and linkages between different processes and risks are understood from the overall context of business impact and consequences to the organization.

One vital component to consider for cyber risk scenario development is the incorporation of systemic risk and contagion risk. This is especially true for organizations such as central banks, since they manage and maintain many of the critical systems and processes that are essential for the continuous functioning of the financial system. Figure 8 depicts the risk scenario structure as described in the sections above.

Figure 8. Risk Scenario Structure



Source: Modified Diagram from ISACA, COBIT 5 for Risk, USA, 2013

Elements of Risk

The process of risk identification needs to include a clear and unobstructed understanding of what constitutes risk to the organization. Therefore, there has to be a documentation and analysis process within the organization that addresses the different elements of risk. These include:

- The impact and consequences of a threat being realized against organizational assets.
- Identified threats against assets
- Vulnerabilities that are associated with threats

It is also worth noting that the organization needs to have a risk evaluation process in place, which covers the whole organization. Risk evaluation is the measurement of risk. When conducting a risk evaluation, the following risk environment variables should be considered:

- The nature, context and criticality of the system being evaluated
- The dependencies and requirements of the system being assessed
- The operational procedures, configuration and management of the system
- Training of the users and administrators
- The effectiveness of controls and monitoring processes of the system and business process
- The method by which data and components are being retired/withdrawn from use

Risk is often the result of a lack of training, rather than a lack of necessary equipment. It can be said that, risk arises from the way that equipment is operated and less from the availability of the right tools and equipment.

Risk Factors

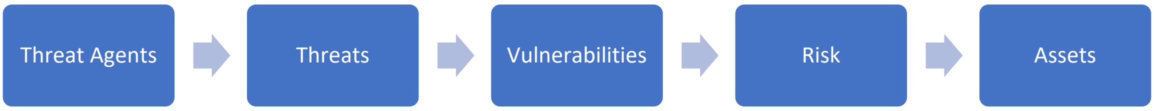
Risk is the result of several factors that interact with each other in order to impact the assets of the organization. The risk factors that pose threats to the organization should be clearly identified and understood. Specifically, risk factors consist of the following components:

- Threat agents

- Threats
- Vulnerabilities
- Risk
- Asset

Threat agents act upon threats to impact the assets of the organization by using vulnerabilities. Figure 9 provides a description of the risk factors that have an impact on the organizational assets.

Figure 9. Risk Factors



Source: ISACA

Assets

The assets of the organization need to be protected. Additionally, the relevant risks associated with assets need to be properly identified. Assets can include:

- People
- Data and information
- Physical property and hardware
- Intellectual property
- Business processes

When dealing with assets, the organization should make sure that all important and critical assets are properly assessed and evaluated. As a result, the organization will be able to determine which assets need to be prioritized in terms of protection. In order to do this, the organization must establish the value of the assets in question. When conducting an asset valuation, the following aspects need to be considered:

- Impact of the asset on existing business processes
- Damage to the reputation of the organization if something adverse were to happen to the asset
- Costs of repair/replacement
- Potential impact on third parties and business partners
- Harm to staff or other individuals
- Violations of privacy
- Breach of contracts
- Legal costs

Threats

Threats can be both internal, or external. The organization should make sure that threats are identified accordingly using a well-established methodology and a set of processes. Threats can be divided into the following types (list is not exhaustive):

- Business disruption and system failure
- Damage to physical assets
- Natural disasters
- Leakage of information
- Unauthorized data modification

In order to determine the nature and type of threats that the organization might face, various sources might be used to gain a good understanding of the threats. These can include other financial institutions, internet service providers, insurance companies, financial regulators and audit reports and publicly available information.

The Incident Response Plan

The following section outlines the main components of an incident response plan that can be used to define the structure and nature of incident response. It includes both technical aspects as well as wider operational risk-related events in its coverage.

An effective incident response mechanism offers considerable benefits to organizations, especially those organizations that constitute (or are assumed to be a part of) critical infrastructure. The incident response plan, if developed and implemented appropriately, would allow the organization to:

- Prevent confusion when an operational event happens. As the former heavyweight boxer Mike Tyson once said, "everyone has a plan, until they get punched in the face."[20] This description applies well to incident response. An organization can have a plan, but if it does not represent reality and is not tested regularly, the effectiveness of the plan can be questioned. On the other hand, if the plan clearly allows the organization to define steps of what needs to be done when a specific event or incident happens, with well-defined roles for response, the existence of such a plan can greatly reduce the impact of an operational event.
- Mitigate the impact of an event relatively quickly. The incident response plan can allow the organization to react in a timely manner and reduce potential costs associated with an incident.
- Establish or re-establish trust with all key stakeholders. A good reputation is key to building trust with stakeholders. An effective incident response plan would allow the organization to maintain a good reputation and establish trust with all relevant entities.

[20] Tyson, M. (n.d.) Everyone Has a Plan Until They Get Punched in the Mouth. Retrieved from https://www.commit.works/everyone-has-a-plan-until-they-get-punched-in-the-mouth/#:~:text=When%20Mike%20Tyson%20was%20asked,first%20contact%20with%20the%20enemy%E2%80%9D.

- Strengthen the overall security posture of the organization. Incident response, especially the kind of incident response that is well-structured and consists of well thought-out scenarios, can enhance the overall security of the organization.

Structure of the Incident Response Plan

The following aspects should be considered when designing and drafting an incident response plan:

1. **Objectives.** The incident response plan should likely include a set of objectives as to what the organization aims to achieve with its incident response.
2. **Strategy.** Following the official definition of objectives, the organization needs to describe the strategy, as to how it intends to achieve the objectives mentioned above.
3. **Policy.** The incident response plan should consist of a clearly defined policy that has been approved by the organization. The policy should describe at a high level, how incident response is supposed to work.
4. **Definition of Events**. Different types of events require different responses. Therefore, the responses should be customized based on the event (incident) that has occurred. The incident response plan should generally not cover only the information technology side of the organization. It should be comprehensive and include different types of operational risk-related events. If needed, a subset of the incident response plan can specifically be created for information technology. The classification of events may include the following:

Event Type	**Definition**	**Activities**
Business disruption and system failure	Events arising from disruption of business or information system failures	Hardware Software Telecommunications Networks Databases Utility Outage / disruptions
Internal Fraud	Losses of a type that are intended to defraud, misappropriate property or circumvent existing company policies, laws and/or regulations by an internal party, such as an employee.	Transactions not reported Unauthorized transactions
External Fraud	Losses due to acts of a type that are intended to defraud, misappropriate property or circumvent existing laws or regulations by an external party.	Hacking damage Theft of information (with monetary loss) Theft/robbery
Damage to Physical Assets	Events arising from the loss or damage to physical assets from natural disasters, or other events.	Natural disaster events Human losses from external events (vandalism, robberies, etc.)

5. **Preparation.** An incident response plan needs to include clearly defined roles and responsibilities for each member of the incident response process.

In addition, communication during incident response is vital. Therefore, incident response should address whether communication can be achieved as needed, during times of need. Incident response plans should include:

   a. Updated contact information of all internal and external responders, or stakeholders, as needed.
   b. Address who will be responsible for incident (event) escalation
   c. Categorizing communications according to priority (i.e. telephone, e-mail, in-person, fax, etc.)
   d. Establishing a certain location for communication and response coordination
   e. Business continuity and the availability of systems during response, including for evidence gathering activities

6. **Detection and Analysis**. Considerable attention needs to be paid to the process of incident detection and analysis. An incident cannot be mitigated, nor addressed, if the organization has not realized that it has been affected by a specific incident. Therefore, there should be relevant detective controls that are able to identify the occurrence of specific events. At the same time, the organization's incident response team and potentially other relevant staff members should have sufficient analytical capabilities in order to analyze what has happened and how to best respond.
7. **Containment, Correction and Recovery.** The organizational incident response plan needs to clearly define risk mitigation actions for the various events that it has prepared for (or at least identified). Factors that can be considered here include:
   a. Evidence gathering
   b. Realized or potential impact of an incident
   c. Resource requirements
   d. How long will it take to recover from an event

8. **Post-Incident Improvement**. This section is (or should be) the lessons learned component of incident response. If something did not work as well as it was intended, then the organization needs to look at the reasons why the process was not effective. Corrective actions should also be determined at this stage, if incident response did not go as intended.

People Risk from a Cyber Perspective

People risk is one of the main sources of operational risk. This includes cyber risk. A risk assessment from the perspective of people risk should incorporate an inherent risk assessment. Inherent risk consists of risk that exists before any controls and risk mitigation practices are implemented by the organization. For example, the financial institution should closely watch and monitor the operational environment of the organization. This is important since it can act as a potential predictor of the kinds of events that the organization might face. For example, if fraud is fairly common occurrence within the financial system, the overall environment has the potential to influence the organization. Likewise, since there is fairly consistent correlation between macroeconomic risk and fraud risk, the macroeconomic environment should also be closely monitored for signs of increasing fraud. This means that if the value of the national currency has been depreciating, or the gross domestic product of the country has been decreasing recently, which has led to an increase of fraud events in the region, the financial institution should assess such risk carefully. The organization can review past fraud events of the financial system (historical losses), if it has access to such information in order to analyze the likelihood of fraud occurring within the organization. In addition, since information systems (technology) plays an ever-increasing role in organizations, the way in which information technology is used by the organization should be assessed closely and in great detail. Large fraud events have happened in the past due to the fact information systems were used to compromise the integrity of data. To summarize, various factors and variables should be incorporated into a financial institution's assessment of people risk.

Hiring and Employment Practices

When hiring, promoting or conducting periodic evaluations of people, financial institutions should consider the following:

- If the position comprises a critical role for the organization, a detailed background assessment should be conducted.

- For subsequent background checks once an employee has been hired, these can be done on a periodic basis for critical employees and roles that require a considerable level of trust. A periodic review can take place once every few years.
- The human resources unit, as well as the business unit of the organization should be responsible for the thorough review of a candidate's/employee's education, employment history, and personal references.
- Incorporation of regular trainings about the organization's values and code of conduct.
- Continuous monitoring and assessment of whether the employee complies with the organization's ethics policy and code of conduct.
- Violations of the ethics policy and code of conduct should be addressed immediately.
- The training of new employees regarding organizational ethics and what the organization expects from the employee should be done as soon as the employee is hired. The process should cover, at a minimum, the topics listed below:
  - The responsibility and obligation to report and communicate certain events internally (and if needed, externally)
  - A list of events, or issues that should be communicated, with specific examples.
  - Information and guidance on how to communicate the issues mentioned above.
  - Fraud awareness should be included in the training process for new employees.

Fraud Risk

Fraud can happen due to a wide variety of reasons and can take many different forms. It can comprise minor employee theft as well as significant financial misstatements and misuse of assets. Factors that can increase the risk of fraud include:

- An operational environment (i.e. financial sector) that has experienced material fraud events in the past, or is especially prone to fraud due to economic, or other reasons
- Lack of an enforceable ethics policy and a code of conduct for employees
- Lack of recognition for job performance and negative feedback
- Ineffective management practices such as a lack of participative management
- Low organizational loyalty levels
- The fear of communicating bad news to management and other key personnel of the organization
- Job compensation that is not as competitive as peers or other organizations in the sector
- Poor communication within the organization
- Insufficient training and promotion opportunities
- Lack of clear organizational lines of responsibility

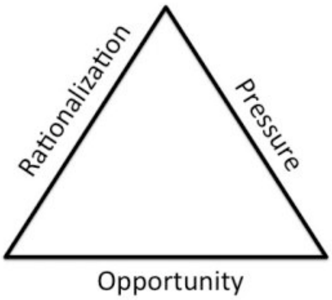
The Fraud Triangle

The fraud triangle is an important aspect of understanding, analyzing and assessing the risk of fraud within the organization. This is due to the fact that many fraud schemes have common characteristics. As a result, the fraud triangle can serve as an effective tool to understand the underlying reasons behind fraud. The fraud triangle includes three components. These are:

- Rationalization
- Pressure
- Opportunity

When it comes to rationalization, the reason why individuals might want to initiate unauthorized activities within the organization is largely due to monetary gain. At the same time, there are other reasons why fraud might happen. These include the desire for authority, revenge and egoism, a factor which is sometimes overlooked when analyzing fraud. It is a general rule of thumb that when monetary gain was not the main goal of the fraud event, the organization should look for other reasons as to why fraud was committed.

Figure 10. Fraud Triangle



Source: http://www.radicalcompliance.com

In order for fraud to occur within the organization, there has to be the relevant opportunity. This is usually and largely due to a lack of adequate and effective internal controls. In some cases, the organization might think that it has effective controls, but if the control mechanisms have not been validated and tested, the control effectiveness can be questioned. If an opportunity to commit unauthorized activity is non-existent, the fraud event itself cannot happen.

There also has to be a component of rationalization based on which an individual decided to initiate the activity. Common reasons might include the following for explaining why someone wanted to be a part of a fraudulent scheme[21]:

- "The organization has a lot of money, so committing fraud was ok."
- "Nobody cared within the organization, so I thought that I could do this."
- "I really needed the money (for medical reasons, loan payments, clothing, jewelry, etc.)."
- "I did not want for my loved one to find out that I had financial issues."

[21] Graham, L. (2015). Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework. Wiley Publishing.

Development of a Fraud Prevention Program

The fraud prevention program consists of three underlying principles. These include:

- The creation of a culture of honesty and integrity
- Fraud risk assessment
    - The creation and implementation of right control mechanisms and processes
- The development of a monitoring program

When it comes to the creation of a culture of honesty and integrity, this should be a top-down approach, since in most cases the employees/staff of the organization follow the example of executive management. So, if the tone at the top is set effectively, this will likely reduce the risk of fraud within the organization. The management should also clearly convey and communicate to the employees what is and is not acceptable behavior. There should also be (or at least it is recommended) that the organization implement a zero-tolerance policy for unethical behavior.

Despite the fact that operational risk is often considered a form of non-financial risk, it can be stated directly that operational risk has significant financial implications. Integrity risk associated with people is one such risk. Not only can integrity risk pose grave consequences to the reputation of a financial institution, but it can also have a large financial impact.

Fraud and the associated integrity risk can take many different forms. It can range from minor infringements of the ethics policy to large fraud events that have the potential to derail, or paralyze an organization's operations, with severe reputational implications. Therefore, financial institutions should have in place a wide-ranging integrity risk and fraud prevention program that is credible and effective. This includes the setting of clear and transparent objectives, as well as the establishment of a relevant strategy. Fraud risk mitigation itself should consist of both preventive and deterrent, as well as detective controls.

Key Point for Consideration:

Many organizations have fairly comprehensive and well-developed policies and instructions for dealing with the ethical conduct of employees. There might also be numerous laws that deal with integrity risks associated with people that demand and specify direct requirements for staff, especially for public servants. This may create a false sense (and illusion) of control.[22] In fact, if such policies and procedures are not directed at actual risks that have been identified in a realistic manner, such control mechanisms might not be nearly as effective as initially intended. Risks should be dealt with in a risk-based manner. Simply complying with procedures, especially when it comes to integrity risk, may create the impression that things are going well, when in reality, both the inherent level of risk, as well as net risk are considerably higher than expected.

Examples of Integrity Risk

Some common forms of integrity risk can include either internal or external fraud (including corruption and collusion), cybercrime (can be considered a part of fraud) and socially unacceptable behavior. Internal fraud is of particular importance in many organizations and can take the form of document forgery, embezzlement, asset theft, or the falsification of financial reports, among others

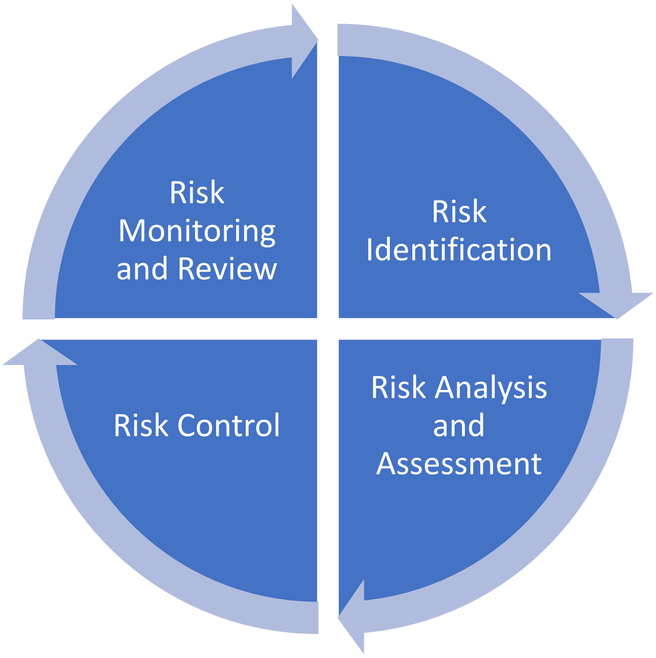
Fraud Risk Management

When an organization develops its strategy for fraud and integrity risk management, the process should cover four key components. These include risk identification, risk analysis and assessment, risk control and risk monitoring and

[22] Source: Dutch Central Bank

review. Figure 11 describes the four phases of integrity risk management, as mentioned above.

Figure 41. Integrity Risk Management Phases



Source: Adapted from the Dutch Central Bank

Unless risks are identified realistically, incorporating in the process all relevant business units and risk managers, the likelihood of not addressing existing inherent risks will be high. The risks should also be analyzed and assessed adequately. Just because a specific event or risk event has not happened within the organization does not mean that such an event will not happen in the future.

It is also worth noting that risk control effectiveness is an inseparable part of integrity risk management. The program itself cannot be effective without relevant internal controls and processes, the aim of which is to prevent unauthorized activity, or actions that might lead to, or result in fraud.

Fraud Risk Prevention Program

The fraud prevention program consists of three underlying principles. These include:

- The creation of a culture of honesty and integrity
- Fraud risk assessment
    - The creation and implementation of right control mechanisms and processes
- The development of a monitoring program

According to Graham[23], before the implementation of a fraud risk prevention program, the following aspects should be considered:

- Does the program cover all of the necessary areas and units of the organization?
- How will the program be implemented?
- Does the program cover all of the necessary/relevant employees?
- How will the program be disseminated and introduced to the employees?
- How will the fraud notification mechanism be set up?

Creation of a Culture of Honesty and Integrity

When it comes to the creation of a culture of honesty and integrity, this should be a top-down approach, since in most cases the employees/staff of the organization follow the example of executive management. So, if the tone at the top is set effectively, this will likely reduce the risk of fraud within the organization. The management should also clearly convey and communicate to the employees what is and is not acceptable behavior. There should also be (or at least it is recommended) that the organization implement a zero-tolerance policy for unethical behavior.

In addition, financial institutions must pay consideration attention to the creation of a positive work environment, with active participation from management. Organizations should have a system of recognition for employees when the

[23] Graham, L. 7. Graham, L. (2015). Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework. Wiley Publishing.

employees perform their job well. Financial institutions should also establish a system of trainings for employees, especially in the area of ethics.

From the perspective of the hiring process, the financial institutions should pay attention to the hiring of individuals that are ethical, have a high level of integrity and are suitable for the position for which they are being hired. For critical roles and positions within the organization, a detailed background check should be conducted. This would include a proper review of the candidates' education and recommendation letters.

A culture of honesty and integrity cannot be created without the support of senior management. Therefore, there should be sufficient assurance that the program has consistent support from senior managers. As a rule of thumb, all staff need to sign the ethics policy. In addition, the bank should assess whether staff clearly understands the ethics policy.

When it comes to discipline, key factors that should be addressed here include how incidents are dealt with. At a minimum, the fraud risk prevention program should include:

- The investigation and analysis of the incident
- Relevant sanctions and actions
- The assessment and potential improvement of controls
- Trainings and follow-up communication

Risk Assessment

One of the first things that should be done is to carry out a risk identification process. The bank should identify possible risks and also determine the nature and the size the risks and what threat they pose to the organization. The organization should assess whether it has relevant processes and control mechanisms via which it can mitigate fraud risk associated with people.

After the risks have been identified, a risk mitigation plan needs to be developed. As a result, subsequent preventive, detective and corrective controls should be implemented. One significant aspect to consider during the risk assessment phase is the size and complexity of the organization, its culture and operational environment. This includes a detailed evaluation of the bank's activities and a review of past fraud events, if such events have occurred before.

While reviewing and assessing internal factors, particular attention should be paid to staff turnover and the movement of employees both within and outside of the organization, infrastructure, and potential problems (as well as inefficiencies) in existing business processes.

The organization, when developing its strategy for dealing with fraud risk, should also establish the type of strategy that should be implemented for dealing with such risks, which includes the following:

- Risk acceptance
- Risk transfer
- Risk mitigation

Subsequently, relevant control mechanisms should be implemented and then monitored for effectiveness. An important question that should be asked at this stage is whether the implemented controls are working as intended.

Figure 12 provides a description of a sample assessment criteria for the effectiveness of controls in terms of fraud integrity risk. Internal control mechanisms should be evaluated regularly to see whether they actually work, or not. If a control has been implemented, but it does not prevent risk from being realized, there really is no reason why such a control should remain within the organization. Therefore, the financial institutions should be vigilant and watchful in the way controls are implemented, and whether they actually work.

Figure 15. Sample Assessment of the Effectiveness of Controls for Fraud Risk

Assessment Criteria for the Effectiveness of Controls	1. Fully operational and fully effective	**Strong:** There are several measures to control risk
	2. Could be improved in certain areas, but the control works adequately and is effective.	**Effective:** Risk is managed sufficiently
	3. Significant improvement is needed, but the control has some effect.	**Ineffective:** Risk is not managed adequately.
	4. No control exists, or the control has no effect	

Source: Adapted from the Dutch Central Bank's Guidance on Integrity Risk

Figure 13 provides a sample risk register for fraud risk. The table identifies the different scenarios that may affect a financial institution and then it lists the likelihood and the impact of an individual scenario on the organization. The risk appetite is also listed in the table in order to illustrate what is potentially acceptable and what is not acceptable for the financial organization in question. For example, if the unauthorized modification of data has a high gross risk, the risk appetite of the given scenario is unacceptable to the financial institution and it must therefore be mitigated.

Figure 13. Sample Risk Register for Integrity Risk

Scenario	Likelihood	Impact	Gross Risk	Risk Appetite
Deliberate Data Leakage	4	4	High	Unacceptable
Unauthorized Modification of Data	4	4	High	Unacceptable
Document Forgery	2	3	Moderate	Acceptable, Monitor
Theft of Property	2	2	Moderate	Acceptable, Monitor

Monitoring

The monitoring of fraud risk management and its effectiveness can be done in different ways. This includes monitoring at the level of the risk management council (board), executive management, the audit committee and external parties that are used for additional assurance (such as external audit). The involvement of internal auditors is vital in this process. The internal audit serves as a powerful mechanism for monitoring the effectiveness of the fraud risk management program. It also has a detective function as well as a deterrent/preventive function by evaluating the sufficiency of internal control mechanisms that are established within the bank.

Stress Tests

Cyber risk stress tests have to be viewed in light of the general operational risk stress testing framework, which is an emerging topic globally that is in a constant process of development. It is important to note that both the financial aspect and non-financial aspects of operational risk need to be stress tested within financial institutions. This means that cyber risk has to be viewed in light of the financial impact that it can have on an organization, along some of the other forms of operational risk. In addition, the non-financial dimension of operational risk, including information technology risk that comes from technological failure and information system disruptions also needs to be considered.

Stress Testing: What is it and its Implications

The main purpose of stress testing is to evaluate the resilience of banks and potentially other financial institutions (intermediaries) in the face of severe but realistic events, including various economic scenarios.

From the perspective of financial regulators, stress tests need to be performed in order to assess potential adverse scenarios to financial stability and how they might impact regulatory decisions. In addition, stress tests can aid financial institutions, including banks to better manage risk within the organization, including for the allocation of capital.

Why Should Stress Tests be Performed?

Financial institutions and regulators should use stress tests as an instrument/tool in order to assess and understand some of the main and emerging risks that might be associated with cyber risk. Cyber risk, when viewed in the context of systemic risk, poses a significant threat to financial stability, unlike many other forms of operational risk, which are generally idiosyncratic in nature.

What Should be Stress Tested?

Stress tests can take various forms. In the context of operational risk, stress tests can be used to develop a model for forecasting potential operational risk events such as those associated with fraud, or conduct risk and the impact that these can have on an organization, including its financial condition. For example, material fraud events can, in some cases, severely hamper an organization's financial condition. In addition, stress tests can specifically cover individual information systems to see how well a critical information system, such as the real-time gross settlement system (RTGS), electronic banking and other widely used system can handle additional transaction volumes/demand from customers during specific time intervals such as holidays, or other similar events.

From a cyber risk perspective, specific stress test scenarios associated with cyber-attacks and technological disruptions need to be developed for stress testing purposes. Furthermore, a cyber-incident need not be directed at a financial institution directly, in order for it to have a potentially adverse effect on a financial institution such as a bank. For example, internet service providers may become the target of a cyber-attack, which indirectly may affect a financial intermediary and cause a shutdown of the financial intermediaries services. The same applies to information technology service providers. If the core banking system is compromised by malware, this also has the potential to adversely affect the banking system indirectly and lead to a significant operational impact (both financial and non-financial).

Operational risk stress tests, therefore, have the following general characteristics:

- Can be a useful tool to assess the impact (both financial and non-financial) of various operational events, including events associated with information technology and cyber risk.
- Similar to scenario analysis, since it estimates the impact of an event on organization, and not its frequency.

- Usually risk factors such as price and volume are stressed beyond normal capacity[24]
- Information systems can be stress tested to see if they can handle increased volumes.
- Can uncover faults in processes and systems that can cause unexpected problems

Penetration tests can also be considered as a part of the overall stress testing framework, since penetration tests often assess vulnerabilities and potential deficiencies associated with an organization's business processes from the perspective of cyber risk and information security. As a result, black box, white box, and grey box testing can all be used as a part of the penetration testing process.

Crisis simulation exercises can also be used to stress test communication and coordination among the various entities throughout the financial system.

When referring specifically to cyber risk, it can be viewed from a wider information security perspective which covers the confidentiality, integrity and availability of both information assets and systems. Furthermore, from an IT risk management perspective, the 4A framework can be used to identify some of the main risks, which can generally be defined as the following:

- Availability: Ensuring that processes (especially critical processes) are operating continuously, without significant interruptions. This also covers the recovery component of operations, including backup measures.
- Access: Making sure that information is protected and that access is granted only to authorized individuals, while unauthorized individuals are denied access.

[24] Hong Kong Banker's Association

- Accuracy: Validating the information that a financial institutions possesses and making sure that the information is accurate and can be provided in a timely manner.
- Agility: Managing information technology-related projects effectively and efficiently.

Cyber risk is a significant, emerging operational risk that requires considerable risk attention.

Communication

When developing operational risk stress tests, including those for information technology, and, especially cyber risk, good, effective and timely communication is one of the more critical aspects of incident response. When looking at this from a NIST framework perspective[25], NIST has dedicated one of the main cybersecurity management functions to incident response. As a result, incident response should be one of the main aspects of many operational risk stress tests, especially those that are related to cyber-incidents, including system disruptions and business failure.

When a specific event happens, financial intermediaries must communicate with different entities and stakeholders internally and externally. Some of the stress tests that can be carried out by regulators and regulated entities, such as banks, should mimic this process. This includes communication both within the various structural units internally, as well as with customers/consumers, other regulatory bodies and government organizations. The process of communicating with customers and media, as well as potentially other stakeholders can be tested within the context of the organizations' business continuity plans.

Dependence on Other Sectors of the Economy

Stress tests, should, at least take into consideration the dependence of the financial system on other sectors of the economy. The financial system is critically

[25] NIST Cybersecurity Framework.

dependent on the energy, telecommunications, information technology and transportation sectors. Operational risk stress tests, should therefore incorporate some of these elements in the scenarios that are developed for stress testing purposes.

Cyber Resilience and Stress Tests

According to the U.S. National Institute of Standards and Technology (NIST), **cyber resilience** is defined *as the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources*[26]. Financial institutions that make up the financial system, especially those institutions that are deemed as being systemically important to the safe and sound functioning of the economy, need to have relevant governance, management and control processes in order to ensure cyber resilience. Furthermore, cyber resilience also needs to include an aspect of stress testing in the wake of adverse or unexpected events. Without a robust stress testing framework, it will be difficult to gain assurance that an organization such as a commercial bank or a credit union will be able to cope with various cyber risk scenarios. It is therefore important to have a holistic approach towards cyber resilience and cyber risk, in general. This is especially true for the financial system, since it forms the backbone of most national economies.

Stress testing is a vital part of cyber resilience. The two main aspects of resilience are to ensure a financial institution's profitability through business continuity and incident response planning. The organizations' business continuity process needs to include the identification of critical business processes, risk assessment, regular testing of business continuity tests and monitoring.

This will allow financial organizations to identify how quickly and effectively they can react to any given scenario that might develop. An important note to point out

[26] Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. & Guissanie, G. (February, 2020). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

is that financial institutions should not rely solely on historical events and losses. As a result, financial institutions need to be forward-looking when they develop their scenarios. Just because an event has not happened in this past, does not guarantee that it will not happen in the future.

This is what cyber risk stress tests should cover. The main precept behind such stress tests is to identify the critical organizational systems, people and locations needed to continue to serve customers on a continuous basis and how to protect and recover the assets.

When conducting cyber risk stress tests for the purposes of cyber resilience, financial institutions must make sure that there is sufficient backing for the process from executive management. As already mentioned above, cyber resilience is a top down process. If there is no commitment from the management of the organization in order to show that cyber resilience is an aspect that the organization pays considerable attention to, there is only a small chance that such processes can succeed. It is consequently vital to ensure backing of both executive and senior management. There should also be sufficient time for testing and validation of the stress test framework.

It is important to identify the goals and objectives of the stress tests that are being conducted. The financial institution must also identify the key people and functions that are critical to the business, in order to prioritize the order in which the processes will be recovered during incident response. This process is generally referred to as incident response. The organization needs to emphasize that all key employees/staff are involved in the stress testing process. These will likely be individuals who perform or supervise the critical operations, as identified during the business impact analysis.

It is worth noting that in some cases, external parties, such as outsourcing service providers, such as technology service providers or organizations that are responsible for incident response, may also be involved in the stress testing process. This can help to identify any potential vulnerabilities or deficiencies that might come from the outside. As a result, the testing process should be comprehensive and involve any, and all relevant people.

When it comes to the development of individual scenarios, an organization can come up with scenarios that are relevant, but slightly beyond the scope and nature of what has happened in the past. In order to make cyber resilience stress testing effective, it is therefore important to cover adverse, but relevant scenarios, that might affect a financial institution. Such a scenario might deal with ransomware that has happened in the financial system, but has not directly affected the financial institution that is conducting the stress test. Other scenarios might include distributed denial-of-service attacks that attempt to bring down an organization's online banking presence, or a phishing attack that has compromised the integrity of an organization's general ledger.

Last, but not least, an effective form of stress testing can include crisis simulation exercises. These can comprise an important aspect of preparedness. While not testing the business continuity processes of an organization directly, crisis simulation exercises can test how well a financial institution may respond to a specific event. The simulation exercises never usually mimic reality fully, but they do allow the participants to rehearse beforehand what an actual event may lead to. Therefore, crisis simulation exercises are a good mechanism to test incident response. They would also allow key decision-makers such as executive management to practice their decision-making skills.

Mitigants

Another significant aspect of stress testing is risk mitigation. While a stress test can tell an organization where deficiencies and inadequate processes exist, it is also necessary to come up with ways to manage the risks that have been identified. These mitigating actions can include the provision of liquidity, emergency cash or extending overdrafts, or granting loans of last resort. This depends on the scenario that is being tested.

Other Considerations (Operational Risk Stress Testing)

When viewed in the wider context of operational risk stress testing, several issues need to be addressed and taken into consideration. Operational risk, and especially cyber risk can be a difficult risk to quantify. In some cases, a qualitative stress test may be the optimal choice, since a quantitative test, such as those that are used for credit and market risk purposes, will not yield a credible test/result.

In the case of cyber risk, the initial impact to an organization might be non-financial in nature, as in the case of a denial of service attack, but can still have a significant negative impact on an organization's profitability, if, for example the financial institution such as a bank is unable to provide essential financial services to its customers.

In general, operational risk stress tests need to be conducted while taking into consideration the overall macroeconomic environment. While this might not pertain to the testing of information systems directly, other forms of operational risk, such as fraud risk may be affected by changes in macroeconomic conditions.

When conducting stress tests, factors such as whether the economy is growing (i.e. GDP is increasing), unemployment is rising, or the value of the local currency depreciating can all have an impact on the financial system's operational risk environment. For example, if unemployment has been increasing recently, which can be correlated with an increase in crime, fraud risk and fraud event may generally rise as well. As a result, the risk of both internal and external fraud may increase. Furthermore, if the economy is experiencing a period of significant economic expansion (growth) the use of credit cards and other plastic cards may rise, due to a rise in consumption, which can increase card-related fraud and other cyber crime.

Scenario Development

Scenario development is critical for effective stress testing. Again, general operational risk scenarios can be used, as well as more detailed and granular scenarios, that might be relevant for a specific financial system. If using a top-down, regulator prescribed stress test, risk managers (also financial regulators) may develop different scenarios that can be classified according to the following categories:

- Liberal – This scenario presents, or has a mild adverse effect on the organization or the financial system in question.
- Adverse – This would be the type of scenario that has a significant impact on the organization being test, or the financial system, but not a severe, or a catastrophic impact.
- Severe – As the term itself implies, a severe adverse impact on the financial institution, or the whole financial system.

For operational risk events, some of the operational losses can be quantified. For example, when dealing with internal and external fraud, as well as various other events such as regulatory fines and the discovery of insufficient funds, such events can be quantified in financial terms. On the other hand, system disruptions and technological failure may have to be modeled in terms of the inability of a specific information system to handle a certain amount of transactions (excessive number of transactions that cannot be processed by the system).

Operational risk stress tests can be carried out in absolute terms, meaning in total projected (forecasted) losses to an individual bank, or financial intermediary, or in terms of the whole financial system. The main objective of such tests would be to determine the total potential operational losses that an individual organization, or financial system would incur. Table 1 presents individual loss scenarios for various operational loss event categories.

Operational risk stress tests can also be carried out for individual operational loss events. This means that either the risk manager, or the financial intermediary would try to determine what the maximum individual loss could be either for the bank (financial intermediary), or for the whole system. The difference here is that only individual losses would be "stress tested" based on a specific scenario such as those listed above (liberal, adverse, severe).

Table 1. Operational Risk Stress Test Individual Loss Scenarios

Individual Loss Scenario				
Loss Event (Event Type)	Maximum Individual Loss (per event)	Liberal	Adverse	Severe
Internal Fraud	1,862,516.00	2,793,774.00	3,725,032.00	5,587,548.00
External Fraud	299,779.00	449,668.50	599,558.00	899,337.00
Clients, Products and Business Practicess	49,905.00	74,857.50	99,810.00	149,715.00
Employment Practices and Workplace Safety	145,187.00	217,780.50	290,374.00	435,561.00
System Disruption, Business Failure	25,391.00	38,086.50	50,782.00	76,173.00
Damage to Physical Assets	13,630.00	20,445.00	27,260.00	40,890.00
Execution, Delivery and Process Management	499,817.00	749,725.50	999,634.00	1,499,451.00
Total	**2,896,225.00**	**4,344,337.50**	**5,792,450.00**	**8,688,675.00**

In the case of information technology, specific information systems can be stress tested in order to see if they can withstand increasing loads of transactions, or client-related requests. For example, a financial institution's internet banking system can be reviewed to determine if the information system can handle an increasing volume of transactions during holidays, or other similar events. The same applies to other relevant systems such as mobile banking, point-of-sale, automated teller machines and other systems. Table 2 provides a sample in the form of a hypothetical scenario of transactions within an internet banking system. Again, liberal, adverse, and severe scenarios are used for forecasting the number of transactions that the system (internet banking system) can handle based on the financial institution's forecast.

Table 2. Information Technology-related Stress Test Simulation for an Internet (online) Banking System.

Date	Actual Transaction Volume	Maximum System Capacity (to Process Transactions)	Liberal Scenario	Adverse Scenario	Severe Scenario
11/1/1995	15750	10000	23625	31500	47250
11/2/1995	8425	10000	12638	16850	25275
11/3/1995	2522	10000	3783	5044	7566
11/4/1995	13464	10000	20196	26928	40392
11/5/1995	15744	10000	23616	31488	47232
11/6/1995	476	10000	714	952	1428
11/7/1995	11423	10000	17135	22846	34269
11/8/1995	12426	10000	18639	24852	37278
11/9/1995	4176	10000	6264	8352	12528
11/10/1995	4534	10000	6801	9068	13602
11/11/1995	711	10000	1067	1422	2133
11/12/1995	5334	10000	8001	10668	16002
11/13/1995	16155	10000	24233	32310	48465
11/14/1995	2441	10000	3662	4882	7323
11/15/1995	1292	10000	1938	2584	3876
11/16/1995	8396	10000	12594	16792	25188

Information Sharing and Analysis – The Case of the ISAC

The financial system forms the backbone of most economies. Setting up an information sharing and analysis center, which has the aim of sharing useful information on various incidents within the financial system can be very beneficial in mitigating both existing and emerging risks. The establishment of such a process should be viewed within the wider context of a public-private partnership between the public and private sector stakeholders of the financial sector.

The information sharing and analysis center (including platform) can potentially be set up either within the financial regulatory authority, or as a separate organization/entity. The main enabler of the information sharing and analysis center is trust. This includes trust from the perspective of financial institutions, as well as the financial regulatory authority (or central bank), that will be involved in sharing the relevant data/information on incidents.

The main objective should be to promote the sharing of relevant and key information about cyber and other operational risk-related events that can be acted upon by the participants of the financial system (such as banks, credit unions, or others). **The information that is shared should be actionable**. This means that, in most cases, the information that is shared should be the kind of information that the participants can readily use to take action, or mitigate risk, in general.

What might be the objectives of an information-sharing and analysis center?

There are several important benefits of setting up an information-sharing and analysis center. These might include:

- Receiving timely information about various incidents and threats that might pertain to the financial system.
- Developing and providing recommendations for mitigating risk around certain events, or vulnerabilities.
- Take preventive steps, as a result of the information that was received in order to increase the resilience of the financial system.

Format and Participants of an Information Sharing Center

The participants of an information sharing and analysis center (ISAC) should include financial institutions. The financial regulatory authority, or a central bank, should also be a key participant and enabler of the information sharing process.

The financial regulator, can in some cases, be the main coordinator and administrator of the information sharing and analysis center. It is also important to consider that the information sharing and analysis center can either be a centralized process, with a single administrator that collects and verifies the content of the information that is to shared, or it can also be decentralized, where members of the ISAC share information directly with each other. In both cases, the accuracy and integrity of the information that is shared is vital. It is usually recommended that there should be an information validation (checking) process before the information is shared with other participants of the ISAC.

Format

Information, with the context of the information sharing and analysis center, can either be shared during face-to-face meetings of financial sector participants, where trust between participants enables the open discussion of various incidents that might pertain to the financial system. As already mentioned earlier, trust is a critical component for the effective functioning of the ISAC, an if trust is lacking between the various participants of the process, the effectiveness of the ISAC will also lower than what was initially intended. **The meetings between the members of the information sharing and analysis center should be regular**. The meetings can either be held quarterly, or more frequently, as needed and dictated by the operational environment and needs of the financial system participants.

Another option is to set up, or develop an information system (i.e. portal) for the exchange of information. This would likely be an electronic information system, where participants of the financial system are granted access to relevant information about incidents that are shared with the participant (members of the electronic platform) in an anonymized manner. **Information regarding incidents should be shared in an anonymized manner, not to reveal the names of specific financial institutions, or in some cases, people/individuals that might be associated with a specific incident, or an operational event.** In certain jurisdictions, it is illegal to share the names of people associated with a specific incident. The financial regulatory authority, or another entity can act as a facilitator or administrator of the electronic portal where information is gathered, or shared. The regulatory authority can also take on the additional responsibility of verifying the data/information that is submitted by the financial sector participants.

In both of the formats mentioned above, it is important for all of the members to at least sign an agreement, such as a non-disclosure agreement (NDA), in order to legally agree on the fact that the information that is shared with the participants (members of the information sharing mechanism), will not be shared with outside/external entities.

The ISACs generally are small organizations, where each participant is expected to share the same level of information as is received. As a result, free-riding, where one or a few members share all, or most of the information, while other members simply receive the information, should be avoided.

In most cases, where an information sharing and analysis center has been set up, there are no membership or commission fees for members.

In addition, in some of the jurisdictions where an information sharing mechanism has been set up, the entry of new members to the information sharing and analysis center requires the unanimous decision of all existing members/participants. Furthermore, there should also be clear rules and guidelines as to what is expected of each member.

Active participation from all members of the ISAC is essential for the information sharing process to work effectively. If there are physical meetings for the facilitation of the ISAC, all participants should be expected to attend the meetings.

Members of the ISAC

The members of the information sharing and analysis center should be risk managers or other experts that are allowed to share sensitive, incident-related information or information about specific operational loss events. These individuals would generally include operational risk or information security managers within financial institutions.

What Information is Shared?

There is a fairly wide variety of information that can be shared within an ISAC. As a general rule though, information only regarding operational (including) cyber risk-related events should be shared, that also includes IT risk-related events such as business disruptions or technical failures. Information regarding credit risk, or market risk, as well as other forms of financial risk that are not directly related to operational risk, should not be shared in an ISAC context.

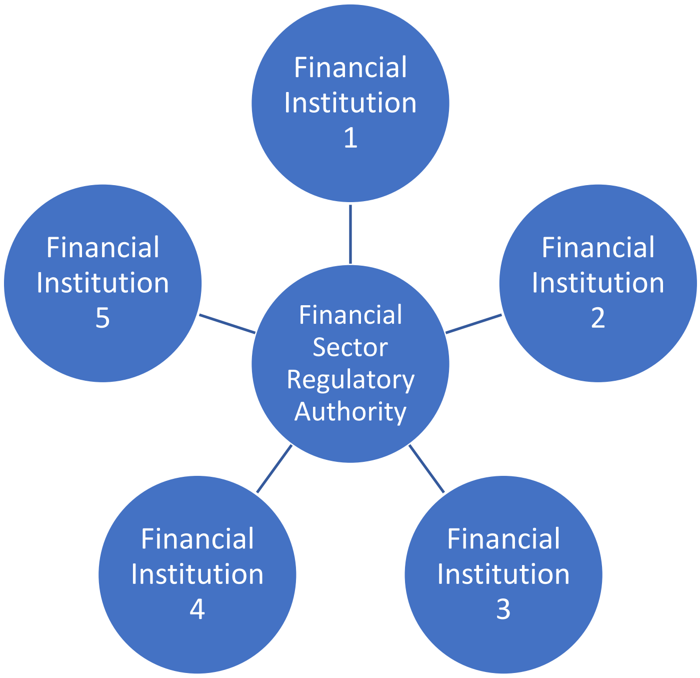
The following information is usually shared within information sharing and analysis centers:

- Incident-specific information on cyber risk-related and operational risk events (although, in some cases, operational risk-related events may not be shared, since this might be too broad).
- Advice and support on how to take protective measures, or mitigate risk
- Information about systemic risk, that may have an impact on the whole financial system
- Alerts on imminent threats to the financial system
- Analysis of incidents and threats that can aid financial institutions in the risk mitigation process
- Technical vulnerabilities that might affect the financial system
- Good practices on incident-handling
- Any other relevant information that can help financial system participants in mitigating risk in a timely manner

It is also worth mentioning that there should be a specific set of rules, or a protocol for sharing information. This can include using the traffic light protocol (TLP) for the sharing of information.

Furthermore, members can use or develop a format for the sharing of incident-related information. The financial regulatory authority (or a central bank) can also require members to submit information on incidents using a specific incident, that might be shared in a sanitize manner, once it is validated by the financial regulatory authority (if the ISAC is centralized and participants do not share information horizontally). Figure 1 presents a diagram for a centralized information sharing and analysis center.

Figure 64. Illustration of a Centralized ISAC



In the diagram above, each financial institution shares incident-related information with the financial sector regulatory authority, who is responsible for aggregating and validating (checking) the information that is received, before it is sent to any of the other participants of the ISAC. Again, it is important to note that incident-related information should be anonymized, before it is shared with any of the other participants of the ISAC. This means that only process-related and technical details should be shared with the participants, and not the names of specific financial institutions (or individuals) that share the information within the context of the ISAC.

Initial Development

When a decision to set up an information sharing mechanism is made, key entities and individuals need to be identified. This means that whoever decides to set up the ISAC, should identify who will be the process owner for the ISAC (i.e. an administrator/facilitator) and who will be the members with the right to share information within the ISAC. During the early stages of the ISAC, it makes sense to involve only a few financial institutions (such as large commercial banks or other, relevant financial institutions), in order to make sure that the process is set up effectively and builds on trust. Again, if there is no trust between participants, it is highly unlikely that useful information will be shared between participants. Whoever takes on the responsibility for setting up the ISAC, should therefore make sure that trust is built into the process of setting up the ISAC from the very initial (developmental) stages of the ISAC.

It is also important to identify and delineate the kind of information that will be shared. A certain taxonomy, or a set of rules should be developed to foster the information exchange process. In most cases, it is not recommended that information be shared in a free format, where it is difficult to classify information based on relevant categories and rules. As a result, a specific lexicon of terms for classification is recommended.

Before an ISAC is set up, all members should be bound by certain rules that govern the operation of an ISAC. This will ensure that each participant understands the responsibility that has been assumed (taken on) by participating in the information exchange mechanism.

Conclusion

Cyber risk is a systemic operational and financial risk. The financial system is especially vulnerable to cyber risk due to its critical dependence on the telecommunications and information technology sectors. As a result, preventive, detective and corrective controls should be used in conjunction with administrative controls to create the kind of defense-in-depth that would allow financial institutions to mitigate cyber risk within acceptable risk tolerance levels. In this regard, financial institutions should pay considerable attention not only to the core cybersecurity control mechanisms that are associated with confidentiality, integrity and availability of data. Considerable emphasis should be placed on cyber resilience processes and how an organization is able to proactively identify cyber risk within its environment. This includes participation in information sharing mechanisms and fora.

It is also worth noting that stress testing is an invaluable component of cyber risk management. Stress tests should be based on specific, realistic scenarios. In addition, stress testing can incorporate penetration tests, vulnerability assessments and crisis simulation exercises (CSEs). In order to gain a maximum benefit from crisis simulation exercises on a system-wide (or national) level, they should not only include the financial regulator, but other entities as well. These might include commercial banks, the Ministry of Finance, CERT, internet providers, and others.

The incident response plan is an additional critical aspect of cyber risk management. The development of an incident response policy just by itself is not enough. If the incident response plan is not tested, there really is no way to know whether the organization can respond effectively to the risk scenarios that have been identified in the incident response framework. Furthermore, the incident response plan needs to incorporate objectives as to what the organization aims to achieve with its incident response. Following the official definition of objectives, the organization needs to describe the strategy in order to describe how it intends to achieve the objectives mentioned above. The incident response plan should consist of a clearly defined policy that has been approved by the organization. The policy should describe at a high level, how incident response is supposed to work and also define a set of events that the financial institution might have to respond to.

To summarize, cyber risk management consists of a multi-pronged approach that incorporates both proactive and detective controls. Cyber risk should be managed differently than most other forms of operational risk, since it is generally not an idiosyncratic risk. Therefore, concentrating on information sharing that is done in a timely manner as well as dedicating sufficient resources to cyber resilience are necessary for effective cyber risk management.

Bibliography

1. Framework for Improving Critical Infrastructure Cybersecurity. (February 12, 2014). National Institute for Standards and Technology – NIST. Retrieved from https://www.nist.gov/system/files/documents/cyberframework/cybersecurity-framework-021214.pdf

2. Hong Kong Banker's Association. *Operational Risk Management*. (2013). Singapore. John Wiley & Sons. Singapore Pte. Ltd.

3. Nadirashvili, K., Papuashvili, D., Razmadze, R. (2020). Quantitative Risk Assessment Approaches to Operational Risk Management. Journal "Economics and Banking". Volume 7. Tbilisi, Georgia.

4. Chernobai, A.S., Rachev, T., & Fabozzi, F.J. (2007). *Operational Risk: A Guide to Basel II Capital Requirements, Models, and Analysis*. Hoboken. John Wiley & Sons, Inc.

5. Westerman, G., & Hunter, R. 2007. IT Risk – Turning Business Threats into Competitive Advantage. Boston, MA: Harvard Business School Press.

6. Papuashvili, D. (2013). Effective Business Continuity Management. Journal "Economics and Banking". Volume 2. Tbilisi, Georgia.
7. Graham, L. (2015). Internal Control Audit and Compliance: Documentation and Testing Under the New COSO Framework. Wiley Publishing.
8. Laudon, K, & Laudon, J. (2012). Management Information Systems: Managing the Digital Firm. Upper Saddle River, NJ: Prentice Hall.

9. ISACA, COBIT 5 for Risk, USA, 2013

10. NIST Special Publication 800-39: Managing Information Security Risk, USA, 2011

11. Risk Supervisory Manual – Operational Risk Management. (n.d.). Hong Kong Monetary Authority. Retrieved from http://www.hkma.gov.hk/media/eng/doc/key-functions/banking-stability/risk management-policy-manual/OR-1.pdf

12. Regulation of the National Bank of Georgia on the Management of Operational Risks at Commercial Banks. (June 13, 2014). National Bank of Georgia. Retrieved from https://www.nbg.gov.ge/uploads/legalacts/supervision/2014/regulation_of_the_national_bank_of_georgia_on_the_management_of_operational_risks_at_commercial_banks.pdf

13. Regulation of the National Bank of Georgia on Cybersecurity Management Framework of Commercial Banks. (March 22, 2019). National Bank of Georgia.

14. Framework for Risk-Focused Supervision of Large Complex Institutions. (August 8, 1997). Federal Reserve System. Retrieved from https://www.federalreserve.gov/boarddocs/srletters/1997/sr9724a1.pdf.

15. Aldasoro, I., Frost, J., Gambacorta, L., Leach, L., & White, D. (November 11, 2020). Cyber risk in the financial sector. Retrieved from https://www.suerf.org/publications/suerf-policy-notes-and-briefs/cyber-risk-in-the-financial-sector/.

16. Integrity Risk Analysis: More where necessary, less where possible. (n.d.). The Dutch Central Bank – Eurosystem. Retrieved from https://www.dnb.nl/media/pfmbzrah/guidance-integrity-risk-analysis-english-version.pdf

17. Ross, R., Pillitteri, V., Dempsey, K., Riddle, M. & Guissanie, G. (February, 2020). Protecting Controlled Unclassified Information in Nonfederal Systems and Organizations. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-171r2.pdf

18. Principles for the Sound Management of Operational Risk. (June 30, 2011). Basel Committee on Banking Supervision. Retrieved from https://www.bis.org/publ/bcbs195.htm

19. Information Security: FFIEC Information Technology Examination Handbook. (September, 2016). Retrieved from https://ithandbook.ffiec.gov/it-booklets/information-security/

20. Business Continuity Management: FFIEC Information Technology Examination Handbook. (November, 2019). Retrieved from https://ithandbook.ffiec.gov/media/2nifgh2b/ffiec_itbooklet_businesscontinuitymanagement_v3.pdf

21. OUTSOURCING TECHNOLOGY SERVICES: FFIEC Information Technology Examination Handbook. (June, 2004). Retrieved from https://ithandbook.ffiec.gov/media/pqtfvxxq/ffiec_itbooklet_outsourcingtechnologyservices.pdf

22. Papuashvili, D. (2023). Cyber Resilience Implications for the Financial System. Business Administration Research Papers. Retrieved from https://barp.openjournals.ge/index.php/barp/article/view/6774

23. Peltier, T. (2010). Information Security Risk Analysis: 3d edition. Boca Raton, FL: Auerbach Publishers.
24. Stallings, W., & Brown, L. 2015). Computer Security – Principles and Practice. 3rd edition.. Upper Saddle River, NJ: Pearson Prentice Hall.
25. McAffee Virtual Criminology Report 2009. (n.d.). Retrieved from http://resources.mcafee.com/content/NACriminologyReport2009NF
26. Cooperative Cyber Defence Centre of Excellence, authors: Tikk E., Kaska K., Rünnimeri K., Kert M., Talihärm A-M., Vihul L. (November, 2008). Cyber Attacks Against Georgia: Legal Lessons Identified.
27. Shakarian, P. (November-December, 2011). The 2008 Russian Cyber Campaign Against Georgia.
28. Hollis D. (January 16, 2011). Cyberwar Case Study: Georgia 2008. Retrieved from Nazario, J. (n.d.) Politically Motivated Denial of Service Attacks.
29. Overview by the US-CCU of the Cyber Campaign Against Georgia in August of 2008. (August, 2009). United States Cyber Consequences Unit.
30. Guidance on Managing Outsourcing Risk. (December 5, 2013). Board of Governors of the Federal Reserve System. Retrieved from https://www.federalreserve.gov/supervisionreg/srletters/sr1319a1.pdf.
31. Internal Control - Comptroller's Handbook. (January, 2001). Office of the Comptroller of the Currency. Retrieved from https://www.occ.gov/publications/publications-by-type/comptrollers-handbook/internal-control/pub-ch-internal-control.pdf
32. Morgan, S. (November 13, 2020). Cybercrime To Cost The World $10.5 Trillion Annually By 2025. Retrieved from https://cybersecurityventures.com/cybercrime-damages-6-trillion-by-2021/
33. Information Sharing and Analysis Centers (ISACs). (n.d.). European Union Agency for Cybersecurity. Retrieved from https://www.enisa.europa.eu/topics/national-cyber-security-strategies/information-sharing
34. Systemic Cyber Risk. (February, 2020). European Systemic Risk Board. Retrieved from https://www.esrb.europa.eu/pub/pdf/reports/esrb.report200219_systemiccyberrisk~101a09685e.en.pdf
35. Kaffenberger, L., & Kopp, E. (September 30, 2019). Cyber Risk Scenarios, the Financial System, and Systemic Risk Assessment. Retrieved from https://carnegieendowment.org/2019/09/30/cyber-risk-scenarios-financial-system-and-systemic-risk-assessment-pub-79911
36. Fell, J., de Vette, N., Gardo, S., Klaus, B., & Wendelborn, J. (November, 2022). Towards a framework for assessing systemic cyber risk. Retrieved

from https://www.ecb.europa.eu/pub/financial-stability/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html.

37. Systemic Cyber Risk Reduction. (n.d.). Retrieved from https://www.cisa.gov/resources-tools/programs/systemic-cyber-risk-reduction.
38. Lee, Y. C. Crisis Simulation Exercises. Retrieved from https://www.itu.int/en/ITUT/extcoop/figisymposium/2019/Documents/Presentations/Yejin_C_Lee_Presentation.pdf
39. Curry, J., & Drage, N. (2020). The Handbook of Cyber Wargames: Wargaming in the 21st Century. The History of Wargaming Project.
40. Papuashvili, D. (2021). Crisis Simulation Exercises (CSEs) - National Bank of Georgia. International Telecommunications Union. Retrieved from https://figi.itu.int/wp-content/uploads/2021/06/6_David-Papuashvili_NBG.CSEs_.DP_.pdf
41. Farha, R., Ivell, T., Sekeris, E. Operational Risk Stress Testing: Emerging Best Practices. Oliver Wyman. Retrieved from https://www.oliverwyman.com/content/dam/oliver-wyman/global/en/2015/dec/OW_Operational-Risk-Stress-Testing.PDF
42. Cooke, I. (July 1, 2017). IS Audit Basics: Audit Programs. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2017/volume-4/is-audit-basics-audit-programs.
43. Cooke, I. (October 30, 2020). IS Audit Basics: Ethics in Information Technology. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2020/volume-6/ethics-in-information-technology.
44. ISACA®, ITAF: A Professional Practices Framework for IS Audit/Assurance, 3rd Edition, USA, 2014.
45. Pfleeger, C. P., & Pfleeger, S. L. (2002). Security in Computing. (3rd Edition). Prentice Hall PTR
46. Michel, B. (April 17, 2017). The Validity of Penetration Tests. Retrieved from https://www.isaca.org/resources/isaca-journal/issues/2017/volume-2/the-validity-of-penetration-tests.
47. Book, L. S. (July 30, 2020). 4 Reasons Why Penetration Testing Is Important. Retrieved from https://www.horangi.com/blog/4-reasons-why-penetration-testing-is-important.
48. Crisanto, J. C., Pelegrini, J. U., Prenio, J. (June 12, 2023). Banks' cyber security - a second generation of regulatory approaches. Retrieved from https://www.bis.org/fsi/publ/insights50.htm

Annex 1. Cyber Risk Self-Assessment Checklist

	Topic
Inventory of Assets (information assets)	
	Note: Risk managers should check to make sure that the data, personnel, devices, systems, and facilities that enable the organization to achieve business purposes are identified and managed consistent with their relative importance to business objectives and the organization's risk strategy.
	Are physical devices inventoried?
	Is the inventory of assets formalized (i.e. is it a formal process)?
	Is the frequency of inventory reviews adequate?
	Is the inventorying of information assets comprehensive? Does it include the location, owner and asset number of devices, among others?
	Are new devices accounted for and added to the inventory accurately and in a timely manner?
	Is automated software being used to detect and identify new devices?
	Inventory of software platforms and applications.
	Is the inventory of applications and software complete? Does it include information such as the version of the application, operating system, vendor and owner?
	Are new applications and software accounted for accurately and in a timely manner?
	Is the frequency of inventory reviews adequate? This means that in some cases, the inventory process could be carried out once every three months, or six months. It is likely that the inventory process should be carried out at least once per year, at a minimum.
	Organizational Communication and Data Flow
	Does the organization maintain accurate and current copies of data flow diagram(s), logical network diagram(s), and/or other diagrams to

	show organizational communication and data flow?
	Cataloging External Information Systems
	Does the organization maintain a list of external information systems?
	Is the list (inventory) of information systems complete and does it include information such as location, third party, owner and other information?
	Are new information systems accounted for and added to the inventory accurately and in a timely manner?
	Is the frequency of inventory reviews adequate?
	Resources (hardware, devices, data and software)
	Does the organization have a data classification program?
	Are key resources such as hardware, devices, data and software classified and prioritized based on criticality and business value?
Roles and Responsibilities	
	Are information security/cybersecurity roles and responsibilities identified?
	Are information security/cybersecurity roles defined?
	Are information security/cybersecurity roles and responsibilities coordinated and aligned with internal roles and external partners? **Note:** The roles and responsibilities may be defined in policies, job descriptions, agreements, RACI charts, hierarchy charts and/or contracts.
	Is there sufficient independence within the information security roles in order to provide adequate separation of duties for critical functions?
	Are controls and incident notification with critical vendors (third parties) addressed properly by the organization (including within its policies)?
Cyber Risk Identification and Management	
	Are information asset vulnerabilities identified and assessed?

	Is vulnerability testing conducted and analyzed on critical organizational assets?
	Is the organization a member of or subscribes to a threat and vulnerability information sharing mechanism (i.e and ISAC)?
	Does the organization have a formal process in place for disseminating threat and vulnerability information to individuals with the knowledge to review the information and the authority to mitigate risk posed to the organization?
	Are threats both internal and external identified and documented?
	Has the organization developed a process to actively monitor and report potential threats?
	After reviewing risk assessments and business impact analysis, are likelihood and potential impacts identified and analyzed for threats?
	Are threats, vulnerabilities, likelihoods and impacts used to determine risk? Note: risk managers should check to see if the risk assessment process identifies potential foreseeable internal and external threats and vulnerabilities, the likelihood and potential damage of those threats, and the sufficiency of controls to mitigate the risk associated with those threats.
	Is the risk management plan designed to accept or reduce risk level in accordance with the organization's risk appetite?
	Are risk management processes established, managed and agreed to by organizational stakeholders?
	Is the risk management process formally documented?
	Is the risk management process updated regularly?
	Is the risk management process repeatable and measurable?
	Does the risk management process have an owner?
	Is the organizational risk tolerance defined and clearly expressed?

	Has the organization defined and approved a cyber risk appetite statement?
Access	
	Do password parameters comply with organizational policy and/or applicable industry requirements?
	Note: Consider the length, complexity, change requirements and history of passwords
	Are password files encrypted and restricted?
	Are network devices restricted by:
	Unique user logon IDs?
	Complex passwords?
	Multifactor authentication?
	Do system administrators for use multifactor authentication instead of single-factor authentication?
	Automatic timeout if left unattended?
	Automatic lockout after repeated failed access attempts?
	Changing default administrative account names and passwords (such as admin or root)?
	Are credentials revoked when an employee leaves?
	After spot-checking accounts (either on-site or via remote inspection), can the risk manager verify that user access is revoked following termination and accounts are deleted according to policy?
	Are access permissions managed, incorporating the principles of least privilege and separation of duties?
	Are user access profiles are consistent with their job functions (based on least privilege)?
	Is network integrity protected, incorporating network segregation where this is appropriate?
Awareness	
	Does the executive managament have a good (or sufficient) understanding of information security and cyber risk?
	Are all employees trained in information security and cyber risk, as needed?

	Are all users/employees trained in accordance with applicable policy, guidance, and/or requirement (e.g., annual cybersecurity training of all employees)?
	Aer training materials updated based on changes in cyberthreat (or information security) environment?
	Do privileged users, such as system and network administrators understand their roles and responsibilities?
	Does the organization have a process to identify privileged users? **Note:** Check to see if, for example critical employees of the institution are identified and accounted for. This must be a formal process and not a verbal, or an ad-hoc identification of employees.
	Are privileged users' roles well defined and are privileged users trained based on their responsibilities?
	Do third-party stakeholders (e.g., suppliers, customers, partners) understand their roles and responsibilities in terms of cyber risk and information security?
	Do third parties comply with cybersecurity responsibilities defined in contracts and agreements?
	Do physical and information security personnel understand their roles and responsibilities?
	Are knowledge and skill levels needed to perform physical and information security duties defined?
	Is specific role-based training assigned based on physical and information security roles and responsibilities?
	Is there a method in place to measure physical and information security personnel's cybersecurity knowledge and understanding against organization requirements?
	Are training and education materials updated to reflect changes in the threat environment?
Data Security	
	Is static data, or data-at-rest protected?

	Is confidential or sensitive data identified on the organization's network (e.g., data classification, risk assessment)?
	Is confidential data secured (e.g., strong encryption as defined by industry best practices) at rest?
	Are mobile devices (e.g., laptops, tablets, removable media) that are used to store confidential data encrypted?
	For data-in-transit:
	Is sensitive information secured (e.g., strong encryption as defined by industry best practices) when transmitted across publicly-accessible networks?
	Are adequate policies in place regarding transmission of confidential or sensitive information via email?
	In terms of training materials, are employees instructed on organization policy regarding data transmission?
	For third parties, are appropriate security controls in place for transmission of sensitive data? Note: This can be evaluated by looking at and reviewing contracts with third parties.
	Are information assets formally managed throughout removal and transfer processes?
	Is there enough capacity to ensure that availability of information systems is maintained?
	Do organization's resources have enough (sufficient) capacity (e.g., disk space, CPU)?
	Has the risk of distributed denial-of-service (DDoS) been addressed and is in line with the organization's risk appetite?
	Are protections against data leaks implemented?
	Are appropriate controls or tools (e.g., data loss prevention) in place to detect or block potential unauthorized or unintentional transmission or removal of confidential data (e.g., email, FTP, USB devices, Telnet)?
	After reviewing information security meeting minutes and information security strategies, is the risk of data loss prevention or exfiltration of

	confidential data being considered by the organization?
	Are integrity checking mechanisms used to verify software, firmware and information integrity?
Information Protection Processes and Procedures	
	Is there a baseline configuration of information technology/industrial control systems that is created and maintained?
	Is there a system development life cycle (SDLC) to manage systems that is implemented? Note: risk managers should get and analyze a copy of the organization's system development life cycle.
	Are configuration change control processes in place?
	Are response plans (incident response and business continuity) and recovery plans (incident recovery and disaster recovery) in place and managed?
	Are response and recovery plans tested?
	Is cybersecurity included in human resources practices?
	Is there a vulnerability management plan that is developed and implemented?
	Does the vulnerability management plan include frequency of vulnerability scanning?
	Does the vulnerability management plan include vulnerabilities identified in other security control assessments?
	Does the vulnerability management plan include procedures for developing remediation of identified vulnerabilities?
Protective Technology	
	Are audit/log records determined, documented, implemented and reviewed in accordance with policy?
	Are audit logs reviewed in a timely manner?
	Are log files being kept in such a manner that logs are not deleted prior to review and/or being backed up?

	Are audit logs and tools protected from unauthorized access, modification and deletion?
	Do log files cover the following:
	Network perimeter (e.g., intrusion dectection systems [IDS], firewalls)?
	Microsoft systems (e.g., Windows event logs)?
	Non-Microsoft systems (e.g., syslog files for Unix/Linux servers, routers, switches)?
	Is removable media protected and is its use restricted according to policy?
	Is access to systems and assets controlled, incorporating the principle of least privilege?
	Are communications and control networks protected?
	Are network perimeter defenses in place (e.g., border router, firewall)?
	Are physical security controls used to prevent unauthorized access to telecommunication systems, etc?
	Are logical network access controls (e.g., VLAN) and technical controls (e.g., encrypting traffic) in place to protect and/or segregate communications networks (e.g., wireless, WAN, LAN, VoIP)?
	Is there a baseline of network operations and expected data flows for users and systems that is established and managed?
	Are detected events analyzed to understand attack targets and methods?
	Are event data aggregated and correlated from multiple sources and sensors?
	Is the impact of events determined?
	Are incident alert thresholds established?
	Are detected events reported in a timely manner to someone with the knowledge and experience to resolve or escalate the event?
	Are escalated events reported to individuals or groups with the appropriate authority to make decisions about the organization's response?
	Are thresholds defined such that an event triggers the appropriate response (e.g., business continuity response, disaster recovery response, incident response, legal response)?

	Is the network monitored to detect potential information security/cybersecurity events?
	Is the physical environment monitored to detect potential cybersecurity events?
	Is employee activity monitored to detect potential cybersecurity events?
	Can an institution detect malicious code?
	Are malicious code controls installed on all applicable systems and network control points?
	Are malicious code controls updated on a regular basis?
	Are malicious code controls configured to perform real-time scanning or periodic scans at regular intervals?
	Are malicious code controls updated?
	Can the institution detect unauthorized mobile code?
	Is external service provider activity monitored to detect potential cybersecurity events?
	Does the institution monitor for unauthorized personnel, connections, devices and software?
	Is event detection information communicated to appropriate entitites/organizations?
	Are detection processes continuously improved?
Response Planning	
	Do employees know their roles and order of operations when a response is needed?
	Are events reported based on established criteria, procedures and requirements?
	Is information shared according to response plans?
	Is there voluntary information sharing that occurs with external stakeholders to achieve broader cybersecurity situational awareness?
Analysis	
	Are notifications from detection systems investigated?
	Is the impact of the incident understood?
	Are forensics performed?
	Is there a process in place to ensure forensics will be performed when needed?
	Are incidents categorized consistent with response plans?

Risk mitigation	
	Are incidents mitigated?
	Are newly identified vulnerabilities mitigated or documented as accepted risk?
	Are response strategies updated?
	Is there a mechanism in place to regularly review, improve, approve and communicate the plans?
Recovery Planning	
	Is the organization's incident recovery plan (include business continuity and disaster recovery) comprehensive?
	Has the organization handled information and cyber risk incidents successfully in the past?
	Do recovery plans incorporate lessons learned?
	Are recovery plans and procedures reviewed, updated and approved on a regular basis or as changes are made to systems and controls?

Annex 2. List of Potential Key Risk Indicators for Cyber and IT Risk Assessment

	Key Risk Indicators for Information Technology and Associated Processes	
	Note: The following document lists and describes key risk indicators for the timely and persistent identification of information technology risk.	
	Name of Indicator	**Description**
	General	
1	Number of IT Projects that Exceeded Budget	The total number of projects related to information technology that have exceeded the budget that has been allocated by the organization.
2	Total Number of Delayed IT Projects	The total number of projects related to information technology that have been delayed
3	Percentage of Delayed IT Projects	The total number of delayed information technology-related (IT) projects, divided by the number of total projects
4	Total Number of IT Projects Canceled	The number of projects related to IT that have been canceled
5	Percentage of IT Projects Canceled	The total number of information technology-related projects that have been canceled, divided by the total number of projects
6	Total Number of Information Systems (Applications) That are Not In Use	The total number of information systems (applications, programs) that are no longer used by the organization, but are still installed within the organization (on servers, workstations, personal devices, etc.)
7	Total Number of Information Systems (Applications) That are No Longer Supported	The total number of information sytems (applications, programs) that the organization is using, but which are no longer supported by the vendor (at least officially).

8	Percentage of Information Systems that are No Longer in Use	The number of information systems that are no longer in use by the organization, divided by the number of total information systems (applications) that the organization has.
9	Number of IT Service Desk Incidents	The number of IT incidents that have been reported to the Service Desk of the organization.
10	Number of Unresolved IT Service Desk Incidents	The number of IT incidents that have been reported to the Service Desk, but have not been resolved, during the reporting period.
	Availability	
1	Number of Materially Significant System Disruptions (All Information Systems)	System disruptions that exceed 30 minutes. This includes all information systems (applications) being used by the organization.
2	System Availability	This indicator measures the amount of time, in minutes that all system are available to authorized users, divided by the total amount of time in minutes, that the system should be available for all authorized users.
3	Number of Instances When Systems Exceeded Capacity Requirements	List the number of instances when the organization's information systems exceeded the capacity that the system is supposed to handle (i.e. exceeds the limits of the system).
4	Percentage of Downtime Due to Scheduled Activities	List, for all information systems, the total amount of downtime, which is measured in minutes, that has been scheduled and used by the IT for scheduled system maintenance activities (as opposed to unplanned downtime) as a percentage of total downtime (planned and unplanned) during the measurement period.

5	Percentage of Downtime Due to Unscheduled Events	List, for all information systems, the total amount of system downtime, which is measured in minutes, that has occurred due to unexpected and unscheduled events, as a percentage of total downtime (planned and unplanned) during the measurement period.
6	Total Number of Critical System Backup Failures	List the total numberof system backup failures that have occurred for critical systems, over the measurement period.
7	Number of Network Disruptions/Outages Due to Internet Service Provider	List the number of network outages/system disruptions that have occurred as a result of the internet service provider. This includes the unavailability of Internet services and other similar events that are directly/indirectly due to the Internet Service Provider.
	Security	
1	Total Number of Information Security Incidents	The total number of all information security incidents that have been identified over the reporting period.
2	Total Number of Attempted Information Security Breaches	The total number of attempted information security breach events over the reporting period.
3	Total Number of Successful Information Security Breaches	List the total number of successful information security breaches over the reporting period.
4	Number of Unauthorized Entry Attempts in the Data Center	The number of physical entry attempts into the data center where servers and other critical information system infrastructure (such as network equipment) is located.

5	Number of Successful Unauthorized Entries in the Data Center	List the number of successful unauthorized entries into the data center. This can be detected/reported by reviewing data center journal logs, camera recordings from the data center, or other control methods.
6	Total Number of Attempted Network Scanning Attacks	List the total number of attempted network scans that were observed during the reporting period.
7	Total Number of Network Disruption Attacks (Denial of Service)	List the total number of network disruption attacks, such as denial of service, or distributed denial of service attacks that were observed during the reporting period.
8	Number of Critical Information Systems Without Updated System Patches	The total number of critical information systems that the organization is using that do not have updated system patches.
9	Number of Information Systems Where Sensitive Data is Stored	The number of information systems where sensitive/confidential data and information is stored.
10	Number of Information Systems Where Sensitive, Client-Related Data/Information is Stored	The number of information systems where sensitive/confidential client-related data and information is stored.
11	Total Number of Systems Where Employees Have Access to Sensitive Data, But Are No Longer in Official Use	List the number of systems that are no longer in official use, but where employees still have access to sensitive/confidential data.
12	Number of Computers Running Unlicensed Software	The total number of computers that the organization uses, that have unlicensed software installed on them.
13	Percentage of Computers Running Unlicensed Software	The number of computers running unlicensed software, divided by the number of computers that the organization uses.
14	Number of Servers Running Unlicensed Software	The total number of servers that the organization uses, running unlicensed software.
15	Percentage of Servers Running Unlicensed Software	The total number of servers running unlicensed software,

		divided by the total number of servers that the organization uses.
16	Number of Computers Not Running Anti-Virus Applications	The total number of computers that the organization uses, that do not have an anti-virus application installed.
17	Percentage of Computers Not Running Anti-Virus Applications	The total number of computers without an anit-virus application, divided by the total number of computers that the organization uses.
18	Number of Servers Not Running Anti-Virus Applications	The total number of servers not running an anti-virus applications. This means that the servers do not have an anti-virus application installed on them.
19	Number of Mobile Devices Not Running Anti-Virus Applications	List the number of mobile devices used by the organization that do not have an anti-virus application installed on them.
20	Number of Computers Without Updated Anti-Virus Definitions	The total number of computers that an organization uses, without an updated anti-virus definition list.
21	Number of Mobile Devices Without Updated Anti-Virus Definitions	The total number of mobile devices that the organization uses, without an updated anti-virus definition list.

Annex 3. Outsourcing Checklist

	Topic
	Does the organization have an **outsourcing strategy** that is formalized? **Note:** This should be a written strategy that the organization uses and not a verbal statement or process
	Does the organization have an **outsourcing policy** that is formalized? **Note**: The policy should be officially approved and signed
	Does management understand the outsourcing strategy and policy?
	Does the organization's strategy on outsourcing include what can and cannot be outsourced?
	Is outsourcing carried out based on, and in accordance with the size and complexity of the organization? **Note:** The outsourcing service that is provided to the financial organization should be sufficient to meet the organization's transactional and other business needs.
	Does the organization maintain a list of outsourced processes and services?
	Is the list of outsourced services updated regularly?
	Are critical functions outsourced?
	Do organization's employees understand outsourcing risks?
	Are foreign-based outsourcing service providers used?
	Is the technology that is being used for outsourcing services considered as high risk (i.e. legacy systems, outdated technology, etc.)?
	Does the organization use cloud computing for critical business processes and services? **Note:** Risk managers should check about the kind of cloud computing model that the organization uses, if cloud computing is used.
	Does the organization's outsourcing policy match how outsourcing is actually managed within the organization?
Outsourcing Selection	
	Are all stakeholders, including both the business and technological side of the organization involved in the outsourcing selection process?

	Are outsourcing requirements properly established before an outsourcing agreement is signed?
	Does the request for proposal (RFP) process adequately include the organization's requirements and its needs?
	Are there due diligence and proper selection requirements in place for outsourcing agreements?
	Does the due diligence process include the assessment of the following:
	Assessment of the outsourcing provider's financial condition?
	Outsourcing provider's reputational risk?
	Control mechanisms of the service provider?
	Disaster recovery and business contuinity plans and relevant tests?
	The potential use of subcontractors by the outsourcing service provider?
Contract Implementation	
	Does the outsourcing agreement/contract contain a service level agreement?
	Are the rights and responsibilities of both parties of the agreement/contract detailed?
	Are the relevant agreement/contract clauses on control and reporting included?
	Ownership of data (who owns the data) clause is included
	Right to audit?
	Confidentiality of data is included in the agreement/contract?
	Business continuity provisions are included
	Are exit strategies included for outsourcing processes?
Monitoring and Control	
	Does the organization have the capability to monitor outsourcing processes?
	Does the organization conduct risk assessments on outsourcing services?
	Are the key conditions of service level agreements (SLAs) being monitored by the organization?
	Are information security risks assessed for outsourcing services?
	Are business continuity risks assessed for outsourcing services?

	Does the organization monitor system disruptions and technical issues associated with outsourced services?
	Does the outsourcing provider have relevant preventive controls for fraud?
	Does the outsourcing provider have relevant detective controls for fraud?
	Does the outsourcing provider conduct regular information systems audits?
	Does the outsourcing provider conduct regular penetration tests?
	Can the organization independently assess and verify the adequacy of information systems audits being carried out by the outsourcing provider? **Note:** The financial organization needs to be able to check whether the information systems audit that is being carried out by the outsourcing provider is sufficient and whether it covers all key aspects of the outsourcing process.

Annex 4. Business Continuity Management

General	
	Does the organization have a business continuity plan?
	Has the business continuity plan been approved by senior (executive) management?
	Is the business continuity plan up-to-date? Note: The business continuity plan of the organization should generally be updated once every year, or when material changes occur in the bank's operating environment and in the services/products that are being offered.
	Has the business continuity plan been communicated to all of the key stakeholders (employees) within the organization?
	Does senior management (board of directors) provide leadership and adequate guidance within the context of business continuity management?
	Is senior management aware of what is covered by the business continuity management plan?
	Does senior management have a good sense of what are the organizatoin's critical business processes? **Note:** In some cases, management either does not have a good understand of the critical business processes that the organization has, or can have either a very narrow or a broad view. For example, in certain organizations which heavily rely on e-mail, management does not view e-mail as a critical services. This is generally considered to be a flaw.
	Does senior management (board of directors) assign business continuity responsibility and accountability?
	Is the business continuity plan tested at least annually? **Note:** This should be a full business continuity test that covers both the evacuation of people, as well as disaster recovery and the recovery of critical functions based on a particular scenario.
	Does the board of directors allocate resources to business continuity (e.g., personnel, time, budget, and training)?

	Does the board of directors oversee that business continuity management is aligned with business strategy and risk appetite?
	Has management defined business continuity roles, responsibilities, and succession plans?
	Has management allocated knowledgeable personnel and sufficient financial resources?
	Has management formed a business continuity committee?
	Has management created a business continuity team?
	Has management validated that business continuity personnel understand their roles?
	Has management established measurable goals against which business continuity performance is assessed?
	Has management designed and implemented a business continuity exercise (testing) strategy?
	Has management confirmed that exercises, tests, and training are comprehensive and consistent with the exercise strategy?
	Has management resolved weaknesses identified in exercises, tests and training?
	Does management meet regularly to discuss policy changes, testing plans, and training?
	Does management assess and update business continuity strategies and plans to reflect the current business conditions and operating environment for continuous improvement?
	Does the organization have an up-to-date list of all key staff that are involved in business continuity management?
	Is the list of all key staff provided to the business continuity team in the form of a contact card or a similar method?
Audit and Independent Review	
	Has the board and senior management engaged audit (or an independent review) to validate the design effectiveness of the business continuity program and whether controls are operating effectively?

	Does the board or management validate and check that the auditor is qualified to carry out the review and is independent of the business continuity or related functions?
	Does audit coverage of business continuity management processes include the following key areas:
	Comprehensiveness and adequacy of the BIA (business impact analysis) and business continuity risk assessment(s)?
	The reliability, adequacy, and effectiveness of continuity and resilience controls?
	The effectiveness of the risk mitigation program?
	Assessment of the business continuity program effectiveness?
Business Impact Analysis (BIA)	
	In order to identify critical business processes, does the management include the following in the process?
	Organizational charts
	Process maps (or work flows)
	Interviews with key personnel
	Network diagrams and topologies
	Data flow diagrams
	Did management inventory the following critical assets and infrastructure on which the business functions depend? These include:
	People
	Hardware
	Software
	Networks
	Cash reserves
	Facilities
	Infrastructure and services provided by third parties
	Does the business impact analysis produce enough information to identify the following:
	Recovery point objectives (RPO)?
	Recovery time objectives (RTO)?
	Maximum tolerable downtime (MTD)?

	Does the business impact analysis identify properly all critical and key processes that the organization has?
Risk assessment	
	Has management identified all potential foreseeable hazard and threats that might pose a risk to the organization?
	Natural disasters such as earthquakes, floods and fires?
	Technological threats such as cyber-attacks?
	Adversarial such as strikes, protests and other threats?
	Does management identify and inventory the following:
	Internal and external assets?
	Types of threats and hazards?
	Existing controls?
	Does the risk assessment include the impact and likelihood of potential disruptive events, including worst-case scenarios?
Risk Mitigation	
	Does the organization have a backup policy and associated procedures?
	Is the backup policy comprehensive and does it address the needs of the organization?
	Does the organization have a disaster recovery plan (for the recovery of IT processes)?
	Does the organization have a geographically diversified secondary data center?
	Does the organization have an evacuation policy and instructions for both staff and clients?
	Do resilience and recovery strategies meet business requirements?
	Has management established exercise and test plans, commensurate with the nature, scale, and complexity of the recovery objectives that address the objectives and expectations of the exercise or test and outline the scenario and any assumptions or constraints that may exist?
	Do the exercise and test plans include the following:
	Identification of roles and responsibilities for participants, support personnel, and observers?

	A consolidated exercise and test schedule that encompasses all objectives?
	Detailed descriptions of objectives and methods?
	Roles and responsibilities for all test participants, including support personnel?
	Does the business continuity plan address the following:
	Coordination with regulatory agencies, law enforcement, and potentially other relevant government entities?
	Simultaneous disruptions of telecommunications and electronic messaging, including between the entity and third-party service providers?
	Crisis or emergency management communication protocols, including the designation ofa spokesperson(s) to communicate with the news media, as appropriate?
Testing	
	Are business continuity tests carried out according to the business continuity plan?
	Are the business continuity tests comprehensive and include evacuation tests, disaster recovery tests and the recovery of critical business processes?
	Are business continuity tests based on specific scenarios?
	Are the testing scenarios adequate and do they reflect the risks that the organization faces?
	Are all key personnel involved in business continuity tests? **Note:** This might include staff such as executive management, treasury, accounting and finance, payments personnel, logistics, and others.
	Do testing scenarios include the following:
	An outage or disruption of the service provider that provides essential internet and other networking services?
	Incident response plans?
	Communication processes with third-party service providers and other stakeholders?
	Cyber events?