# Framework for managing information security risk and building information resilience through risk based control implementation

("Information Security and Resilience Framework")

Finance Sector Computer Security Incident Response Team (FINCSIRT)

Version 1.0

6/18/2019

# Acknowledgements

This document is the outcome of the ongoing efforts of the Financial Sector Computer Security Incident Response Team (FinCSIRT), to convey the importance of the information resilience to the business and enable the smooth implementation of the information security initiatives in a more transparent, effective, and efficient manner whilst increasing focus towards the achievement of the unique set of business goals and objectives.

The framework is formulated with the knowledge and experience gained over the years by the FinCSIRT as well as the industry best practices, standards, guidelines and frameworks such as ISO, NIST, SANS, CIS, OWASP…etc. The document is published as a framework that assists the business to effectively manage information security risks while strengthening the business information resiliency levels. This framework complements other industry best practices, standards, guidelines and frameworks such as ISO, NIST, SANS, CIS, OWASP…etc. that are issued pertaining to information security (including cybersecurity).

All Information Security experts and businesses are invited to adopt the framework and send us their respective feedback and experience via **feedback@fincsrit.lk**. Any queries and implementation assistance requirements are to be forwarded to **manager@fincsirt.lk** so the said framework can be further improved.

FinCSIRT offers its gratitude to all who have contributed in reviewing the draft documents to assist in the building of this framework up to an acceptable standard. Furthermore, thanking in advance to all who will contribute to help perfect the framework.

# FinCSIRT

FinCSIRT is a project initiated by the Central Bank of Sri Lanka (CBSL) and the Sri Lanka CERT | CC, where LankaClear Pvt Ltd was brought on board to host FinCSIRT as an independent unit by taking up the responsibility of the information security efforts for the Sri Lankan financial sector. LankaClear is the operator of Sri Lanka's National Payment Network and is owned by the CBSL along with other licensed public and private Commercial Banks operating in the nation. FinCSIRT operates its own IT infrastructure and follows strict information sharing protocols and access so that confidentiality of the 45 member Financial Institutes (FI) are maintained while serving.

FinCSIRT provides set of standard services to its members while providing a number of value addition elements, targeting the below three aspects to build the information resiliency within the Sri Lankan financial sector while the experience gathered is shared globally for the betterment of the global information security efforts.

**Targeting Aspects:**

- Sector Information Security Development
- Individual FI Information Security Development
- Global Information Security Development

"Information Security and Resilience Framework" is one of the key initiatives that the FinCSIRT formulated to ensure the local and global development of information resilience of the business against the rapidly advancing information security threat landscape.

FinCSIRT is currently working with entities such as: Central Bank of Sri Lanka, Sri Lanka CERT | CC and LankaClear Pvt Ltd; 45 financial institutes including Banks, Finance companies and Primary Dealers; Global CERTs, CSIRTs and other globally interested parties and vendors to build sector resilience and to contribute to the global information security and resiliency development.

# Executive Summary

Importance of the information is primarily due to the fact that it enables businesses to achieve its goals and objectives irrespective of the business size, industry or the country. With the rapid advancement of the technology and its complexity, information and data (hereinafter referred to as information) security threat landscape becomes wider, thus increasing the likelihood of the businesses to face threats that will impose a significant impact towards achieving the business goals and objectives, which then might even result in a business shut-down.

Likelihood of the threats succeeding becomes more certain and the impact would be intolerable, if businesses fail to identify the risks these threats impose towards the business goals and objectives beforehand and take necessary steps on managing/reducing the impact and the likelihood up to a level which the organization can bare.

Due to this reason, businesses, most importantly the Board/CEO/Owner/Top Management, should have a clear idea of its information security and resilience strategy, and analyse to see if it answers the following questions and to what level:

- What are the set of information the business have?
- What is the information security threat landscape towards business goals and objectives?
- What is its effect on business resilience?
- Has the business identified/defined its risk absorption level/target risk profile?
- What are the current measures in place to manage the rapidly evolving information security threat landscape?
- What risks do the current controls address?
- Has the implemented controls kept the organization under its target risk profile?
- Do the current controls disrupt the business processes?
- Does the business have mechanisms to monitor and revise the current controls?
- Does the business have any clear ROI from the current controls?
- Are there more gaps to be addressed?
- Is the risks identified communicated to the top without any disruption; do the top personnel have enough information and awareness to make risk awareness decisions?
- Does the business have mechanisms to identify business risk profile changes?
- Does the business have a mechanism to continuously monitor, review and implement information security and resilience controls as required?

With the recent developments, businesses have already identified information security as an enterprise risk and begun to have the relevant controls in place. As a boost to the organisation initiatives, the Financial Sector Computer Security Incident Response Team (FinCSIRT) introduces the “Framework for

Managing Information Security Risk and Building Information Resilience through Risk Based Control Implementation" (hereinafter refers to as "Information Security and Resilience Framework") that is to be incorporated into the business. This will in-turn allow the business to strategically manage information security risk in a manner that would support the business's ability to withstand and quickly recover from possible information security threats that disrupts it from achieving its goals and objectives allowing more transparent view of its return on its information security and resilience investments. This can be achieved while addressing aspects not limited to the aforementioned areas and whilst enabling the business to make informed-risk aware decisions.

'The Information Security and Resilience Framework' is designed to be implemented in two layers; Foundation layer and the Structure Layer.

The foundation layer will set the governing framework and course for its information security implementation and resilience to be built with a common vision of enabling the business to achieve its set goals and objectives while managing the information security threat landscape and building organizational information resilience capabilities.

The Structure layer will guide the business to identify the risks, analyse, evaluate, implement the relevant controls, monitor, communicate and continuously review/revise and improve in accordance with the core framework that is set at the foundation layer.

The framework focuses the business towards information security concepts (but not limited to) such as; processes level risk identification, data and data state level risk identification, business environment based risk identification, risk based control implementation, business continuity, policy and procedure base enforcement, Board/CXO's/Owner level interference, criticality and priority based effective control implementation, to ensure information security best practices are followed during the implementation.

The framework is designed to complement any business irrespective of the size, industry or the country. By adopting the framework, it enables the business to minimize the business risk by building the information resiliency and strengthening the information security while facilitating better return on the control investments, better communication of information security and resilience risks, continuous documentation, ability to obtain quality evidences, risk aware decision making, swift compliance with information security industry best practices, standards, guidelines, framework (E.g. ISO, NIST, SANS, CIS, OWASP…etc.) and regulatory requirements and create value addition to the business.

FinCSIRT will ensure maintenance of the 'The Information Security and Resilience Framework' as a continuously fine-tuned and developed framework by closely working with the implementers and the industry professionals to ensure it is up-to-date and compliments all businesses while keeping up with the changing nature of the information threat landscape and resilience requirements.

As an implementation assistance of the framework implementation, this document contains minimum requirements a company should start with while giving suggested implementation methods.

# Table of Content

**Acknowledgements** ---- **i**

**FinCSIRT** ---- **ii**

**Executive Summary** ---- **iii**

**1. Framework Introduction** ---- **2**

1.1. Framework Goals ---- 3

1.2. Benefits of using the framework ---- 3

**2. Framework** ---- **4**

2.1. Foundation Layer ---- 4

2.2. Structure Layer ---- 7

**3. How to use the framework** ---- **12**

3.1. Information Risk Profile ---- 13

3.2. Identification of the Risk Scenarios ---- 13

3.3. Analysis of the Risk Scenarios ---- 14

3.4. Selecting Controls to implement/improve ---- 14

3.5. Setting metrics ---- 15

3.6. Monitor, revise, review and improve ---- 16

3.7. Analyzing the controls effectiveness and efficiency ---- 16

3.8. Adding value to the business ---- 16

3.9. Building a risk aware culture ---- 17

**4. Annexure A - Suggested Steps on framework implementation** ---- **18**

**5. Annexure B : Definitions** ---- **21**

**6. Annexure C : Acronyms** ---- **22**

# 1. Framework Introduction

Information is crucial for the business as it drives the entity to achieve its goals and objectives, irrespective of the business size, industry or the country. Therefore, safeguarding (but not limited to) confidentiality, integrity and availability (CIA) of the information and its related systems from unauthorised access, use, misuse, disclosure, disruption, modification, or destruction, and developing the business ability to withstand and swiftly recover from the incidents, plays a major role in ensuring the timely achievements of the business goals and the objectives.

Information security risk includes, but is not limited to risks that are attached with the instances (E.g. processes, devices, servers, computers and storage areas and etc.) and states (Digital and Physical forms) it is been used, stored, processed and transmitted. These risks should be effectively managed by considering the confidentiality, availability and the integrity requirements the business has for the pertaining information.

CIA triad is considered to be the foundation for information security, although with the time many modals have been built on top of it. When looking at how exactly the CIA triad affects the business;

- Confidentiality, binds with who has access to the information. Disclosure of the information to unauthorised parties would affect the business negatively.
- Integrity, binds with information modification. Unauthorised modification may lead the business to make incorrect decisions and produce falsified outputs incurring the business.
- Availability, binds with the information availability to the authorized parties when required. Any non-availability of the information when required would negatively affect the processes, goals and objectives being timely achieved.

Overall considered, any negative effect on the CIA triad, the business will be faced with a situation of loosing customer trust, legal issues, compliance issues, reduction in market share, negative affect on profit, threat to goals and objectives and even might lead to company shut down.

FinCSIRT introduces the “Framework for managing information security risk and building information resilience through risk based control implementation” (hereinafter referred to as “Information Security and Resilience Framework”) to strategically manage information security risk in a manner that would support the business’s ability to withstand and quickly recover from possible information security threats that disrupts the business from achieving its goals and objectives while allowing the business to have a clear view of the aforementioned aspects. While most the business has taken up the information security and resilience as a thriving enterprise risk, this framework will enable more perspective for development.

The framework focuses the business towards information security concepts (not limited to) such as processes level risk identification, data and data state level risk identification, risk based control implementation, business continuity, policy and procedure base enforcement, Board/CXO’s /Owner level interference, criticality and priority based effective control implementation to ensure information security best practices are followed during the implementation.

The framework is designed to complement any business irrespective of the size, industry or the country. By adopting the framework, it enables the business to minimize the business risk by building the information resiliency and strengthening the information security. All while facilitating better return on the control investments, better communication of information security and resilience risks, continuous

documentation, ability to obtain quality evidences, risk aware decision making, swift compliance with information security industry best practices, standards, guidelines, framework (E.g. ISO, NIST, SANS, CIS, OWASP…etc.) and regulatory requirements and create value addition to the business.

## 1.1. Framework Goals

Framework is built to enable the business to achieve the following goals:

- Complying with information security best practices, standards, frameworks, regulatory (E.g. ISO, NIST, SANS, CIS, OWASP…etc.) and compliance requirements, amongst others.
- Identify the current business status in terms of information security.
- Identify the target business status in terms of information security.
- Minimize the business risk by continuously building the business information resiliency and security.
- Implement risk based controls in the organization effectively and efficiently in a transparent manner.
- Enable better communication of information security risks.
- Enable informed decision making.
- Enable better return on the information security investments to the business.
- Create/Enhance value to the business.

## 1.2. Benefits of using the framework

By implementing information security in accordance with the framework, it offers the following benefits to the business;

- Enables informed, risk based decision making.
- Higher cost benefit/return on investment (ROI) from the information security investments.
- Clear focus on the business goals and objectives.
- Clear identification of what the business has.
- Clear identification of the information security and resilience risk profile.
- Clear identification of the target information security and resilience risk profile.
- Enables effective control implementation for the business.
- Continuous monitoring of the environment, risk profile, implemented controls, Information Security and Resilience Framework of the business and the strategy.
- Continuous improvement of the business information resilience.

- Ensure proactive and reactive measures are in place to assist the continuity of the business.
- Clear and continuous communication paths are built.
- Availability of the clear and continuous documentation.
- Transparency on the clear roles and responsibilities.
- Ease on being compliant with information security regulatory requirements, mandates, best practices, standards, frameworks…etc. (E.g. ISO, NIST, SANS, CIS…etc).

## 2. Framework

Framework consist of two interconnected layers as illustrated on the Figure 1; foundation layer and the structure layer, allowing the business to build a solid foundation to implement its information security initiatives according to the business needs enabling the business to achieve its goals and objectives continuously.

In order to provide better insight on how to implement the framework on necessary aspects, is discussed further on topic 3 (How to Implement the Framework) and suggested implementation flow is as defined on Annexure A.

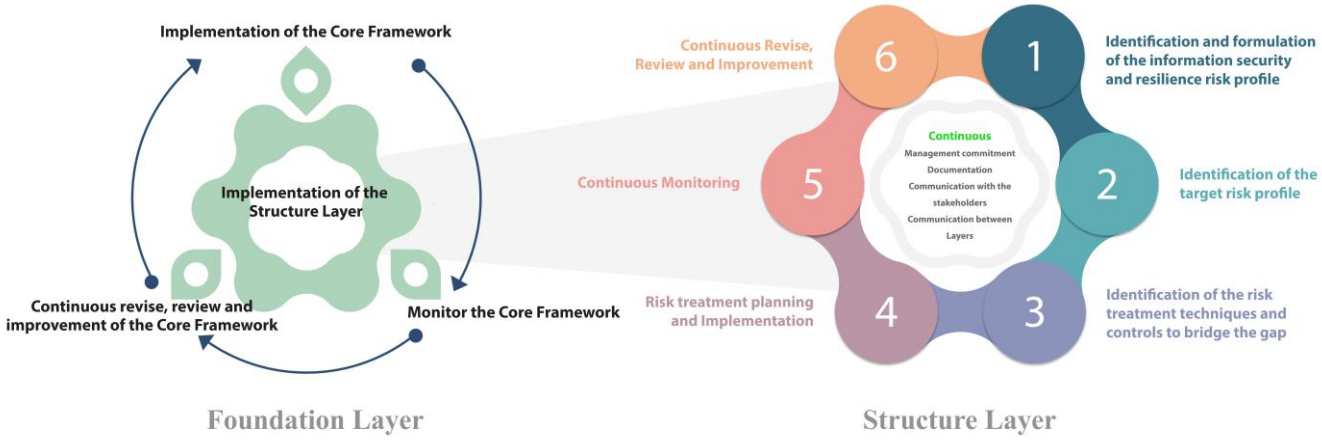


**Figure 1: Information Security and Resilience Framework**

### 2.1. Foundation Layer

Foundation layer will guide the business to set the base for the entire operation by guiding the business to implement its unique governance structure that ensures the structure layer implementations and operations are in line with the organizational goals and objectives.

The governance structure (hereinafter in refers to as Core Framework) will set the tone from the top and it would ensure that the process will not die over the time. This further ensures that the proper management commitment is provided for the successful and continuous implementation and the operation of the structure layer, while enabling documentation and communication throughout the cycle.

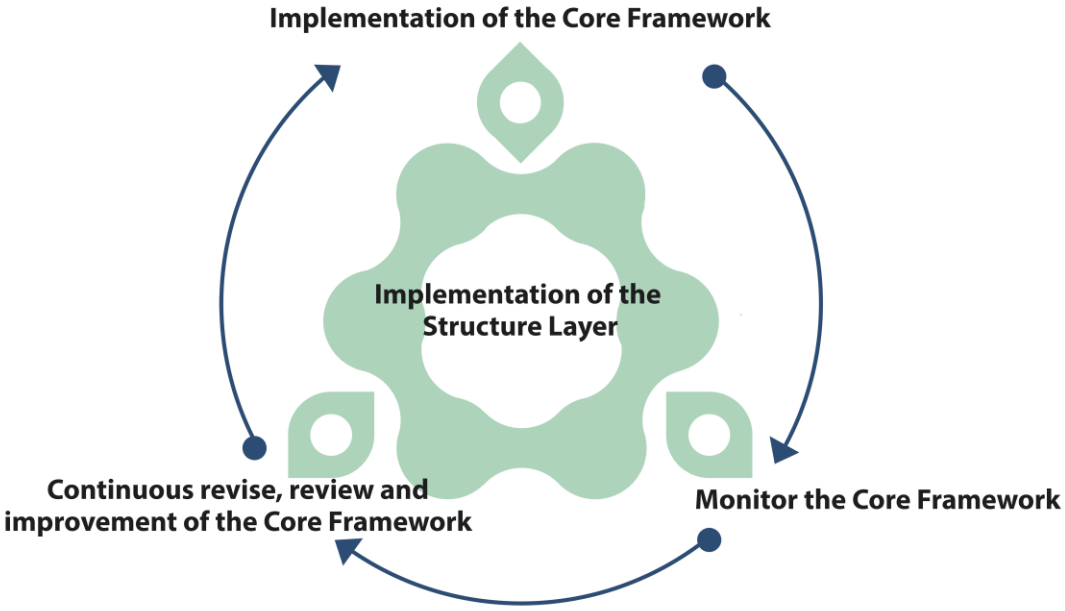


**Figure 2: Information Security and Resilience Framework: Foundation Layer**

## Foundation Layer Components

As illustrated on the Figure 2, Foundation layer consist of four interrelated components.

1. **Implementation of the Core Framework** must achieve/have following five elements:

   - **Appointing a C-level position who has direct reporting line to the Board/CEO/Owner pertaining to information security (E.g.: Chief Information Security Officer)**

     A C-Level person with swift decision making power needs be appointed with a reporting line directly to the Board/CEO/Owner to communicate clearly about the information security issues in order to build Board/CEO/Owner level awareness and assist them to make risk aware decisions.

     Information Security being one of the crucial aspects that needs to be addressed, the appointed person will need to collaboratively work with risk, IT, operations and all other departments to build information resiliency throughout the entire organization.

     CISO role should be able to establish and drive the information security of the company with the assistance of the risk and the governance/compliance teams pertaining to information

security, while internal information security audit team will be independently audit/observe its work and assist identifying the abnormalities/improvement areas.

- **Formal Board/CEO/Owner (Ultimate Risk Owner) level statement issuing full support for the information resiliency building**

  With the importance that is rapidly on the rise on information security being a threat to the organizational goals and objectives, it has become a Board/CEO/Owner level concern that need to be observed and taken action on strategically. Furthermore, Board/CEO/Owner level support is crucial to receive the necessary support from the management and the employees. Therefore, Board/CEO/Owner should issue a formal statement affirming support for the information security initiatives of the business.

- **Defining clear roles and responsibilities**

  Responsibility, Accountability, whom to Consult and who to Inform (RACI) must be clearly defined for the core framework operations, which includes the implementation and operation of the structure layer (Specific control implementations may define at the structure layer with the operations).

  This includes the clear roles and responsibilities inside the organization and as well as out. Especially with the incident responders and the third-party service providers who assist the organization in crisis as well as to keep the day to day operations.

  It must be signed off by the Board/CEO/Owner showing support and must be communicated to the relevant parties (obtain formal acknowledgement) to adhere.

  Board/CEO/Owner may delegate risk acceptance levels and risk based decision making to the top management/committees and the C-Level positions created based on the business requirements.

- **Define the metrics**

  Metrics must be defined to measure the performance and to indicate risks pertaining to the overall Information Security and Resilience Framework (foundation layer and the structure layer). Metrics must be realistic, timely and measurable. Control specific metrics may be defined at the structure layer implementations. These metrics must include the monitoring criteria, communication requirement and the timelines.

- **Formulate the policies and procedures to achieve common direction**

  Policies and procedures pertaining to the Information Security and Resilience Framework (foundation layer and the structure layer) must be defined to ensure the efforts are all focused on a common direction i.e. achieving the business goals and objectives. It must include at minimum the roles and responsibilities, metrics, approval requirements and the documentation requirements. These documents should be version controlled and must be approved by the Board/CEO/Owner and communicated to the relevant personnel.

  It is important to set clear approval process and review periods for the core framework policies and procedures, as well as the structure layer policies and procedures to ensure the continuity.

Furthermore, business should also drive towards implementing a risk aware culture through the policies and procedures which would facilitate better communication, sharing of knowledge and best practices, continuous improvement and employee commitment towards business goals and objectives.

Most importantly, policies and procedures set by the company should be the enablers of the business processes, which adds more value and resilience.

2. **Implementation of the Structure Layer** needs to be carried in accordance with the core framework that is built uniquely to the business, focusing on the business goals and objectives. How it should be built implemented is discussed further on the point 2.2 (structure layer).
3. **Monitor the Core Framework** based on the defined metrics, it should identify any areas for improvement or abnormalities that require attention on the overall process. Its progress and the risk levels must be monitored continuously and communicated to the responsible parties as defined in the policies for the necessary actions.
4. **Continuous revise, review and improvement of the Core Framework** based on the monitoring evidences and the changes in the environment. This step ensures the continuous improvement of the entire process and reassures the process is in the set path. Any revision must be documented on the relevant policy and procedures, approved and must be ensured that the enforcement is reflected throughout the foundation layer.

## 2.2. Structure Layer

The Structure layer will guide the business to manage its information security threat landscape and build its information resilience, efficiently, effectively, transparently and continuously through the risk identification and risk based control implementation as illustrated on the Figure 3.

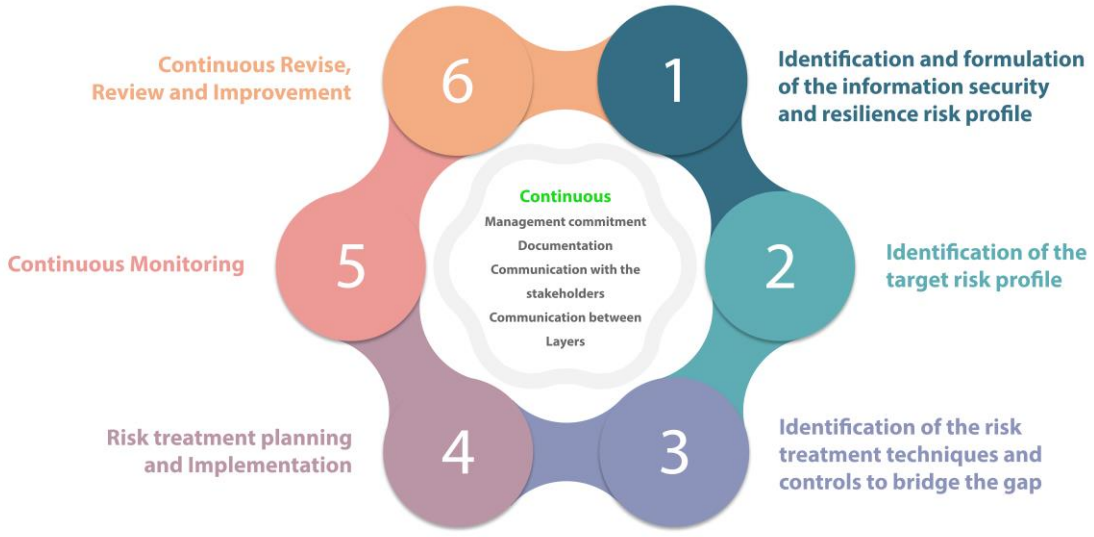


**Figure 3: Information Security and Resilience Framework: Structure Layer**

**Structure Layer Components**

The Structure layer contains two main Components; Circular component and the Mandatory component.

### 2.2.1. Circular component

Ensures the implementation of the information security is continuous and is aligned to the business goals and objectives. Component consists of six sub-components working in a flow.

1. **Identification and formulation of the information security and resilience risk profile**

   Building up the information security and resilience risk profile enables the business to understand about itself, its' surrounding, parties interested, their access to the business data, and help identify the possible risk scenarios that may disrupt the business from achieving its goals and objectives.

   The profile will illustrate a clear picture enabling the business to understand where it stands and what it should do in order to build the information security and resilience capabilities.

   When formulating the risk profile, business needs to identify at minimum (but not limited to) its internal and external environment, its processes, sub processes, technologies, locations and people, along with the pertaining information, its conditions (used, transmitted, process, stored), its forms (digital/physical), its legal/compliance requirements, its resilience requirements, parties interested and parties with access. All such need to be gathered and documented.

   Risk scenarios (RS) can be created based on the identified information with the characteristics such as; realistic, relevant, impact/loss can be quantifiable (E.g.: High, Low, Medium or in Figures), probability can be defined (E.g.: Probable, Highly Probable, Minor Probability or in Figure) and (if possible) time bounded (When is it expected to occur).

   The identified risk scenarios thereafter must be analysed to understand the impact/loss and the likelihood of occurrence.

   Finally, risk scenarios must be prioritised, and if possible grouped. Businesses should use at minimum (but not limited to) the following factors when prioritising and grouping:

   - Criticality of the process/data to the business
   - Impact that the risk scenario may cause
   - Likelihood of the risk scenario
   - Time expected to occur of the risk scenario

   To effectively identify the possible risk scenarios, impacts and the likelihoods, businesses will have to work with different stakeholders, such as (at minimum) legal, finance, risk departments and process owners.

   Documentation: The identified information must be documented whereas the identified risk scenarios must be documented on the risk registry.

**2. Identification of the target risk profile**

Target information security and resilience risk profile, in other terms business risk appetite, needs to be recognized for the each identified risk scenario. This is a crucial step as it shows the risks the business is willing to take in order to achieve its goals and objectives. Clear identification of the target risk profile will enable the business to take informed and risk-based decisions, and invest mindfully so that there will not be any waste of money, time and resources.

Risk appetite must be decided for the each individual risk scenario (business may choose to decide for individual or similar groups of risk scenarios) and have it approved by the relevant authority as mentioned on the core framework.

Documentation: Update the risk registry.

**3. Identification of the risk treatment techniques and controls to bridge the gap**

As the current and the target profiles are known by now, business can identify the gaps and invest on the initiatives strategically. It must keep in mind that the implementation should lead to successful managing of the information security risk while enabling and improving the information resilience of the organization.

Each identified risk scenario must be analysed to see if the current level of risk deviates from the target risk level. If deviations do not exists, further risk reduction is not necessary unless the business requires it. However, if deviations exists, the business is required to choose one or more risk treatment techniques (Accept, Avoid, Mitigate and/or Transfer) to minimize the gap.

These treatment techniques are required to be further analysed to understand the possible treatment categories/options (E.g.: Limit user access, Minimize data leak, log analysing...etc.) available and the controls (E.g.: Employee awareness workshop, Firewall, Active Directory, Privilege Access Management...etc.) available under each category/option.

When identifying the controls, businesses need to first determine: the applicability and the suitability for the business; mechanisms available to monitor the required benefits; proactive and reactive control requirements; and the compliance/legal and resilience requirements.

The identified risk treatment techniques, categories/options and controls required must be prioritised to each risk scenario, and then be documented and approved by the relevant authority as mentioned on the core framework.

Documentation**:** Update risk registry | Gap Document | Prioritised list of risk treatment techniques and controls to each risk scenario.

**4. Risk treatment planning and implementation**

Based on the prioritised risk scenarios, risk treatment techniques and controls, the business can plan the implementation process; allocate resources and responsibilities, and set deadlines and metrics which would allow the business to make use of the limited resources more effectively and efficiently.

These plans may be categorised based on the criticality of the implementations, or as business requires. However, the following must be available whenever any control implementation is to take place:

- Approved business case stating at minimum (but not limited to) the risk, expected benefit and cost.
- Defined metrics (Key performance indicators, Key risk indicators and Key control indicators). Metrics must be realistic, timely and measurable and it must have defined monitoring mechanisms and the timelines.
- Policies and procedures must be implemented/updated with, at minimum (but not limited to) control implementation, maintenance, monitoring, metrics, enforcement and the roles and responsibilities.

Implementation must be carried out based on the set policies and procedures and it must be communicated and the progress must be updated to the relevant parties at defined intervals. If any deviations or any alterations are required, and these policies/procedures and/or metrics need to be updated, it should be done under the approvals of the defined authorities. It is suggested that the implementation is made more efficient and effective; Businesses could make use of project management strategies to conduct the implementations and work on set timelines.

Documentation: Update risk registry | Project plan and the business case | Updated/implemented policies and procedures

**5. Continuous monitoring**

Continuous Monitoring enables the business to observe and enhance the current controls, risk profile, core framework efficiency and the effectiveness. It further provides the opportunity to identify the return on the information security investments followed by clear evidences.

Monitoring must be carried out to ensure the controls are implemented, working, maintained and adhered to, and as well to monitor the set metrics. Additionally, businesses must ensure Control performance, Control efficiency to reduce the risk, Risk Scenario changes, Risk Profile changes and Structure layer performance is monitored continuously.

Any new systems/processes or any initiative of the business monitoring must be captured under the structure layer monitoring and should be reflected throughout the cycle.

These monitored results must be effectively communicated to the relevant personnel as mentioned on the core framework for the reviewing, revising and improving the control and the process.

Documentation: Update risk registry | Monitoring logs | Monitoring reports | Communication Logs

**6. Continuous revise, review and improvement**

As information security is a continuous effort, the steps of Revise, Review and Improvement provides the business with the capability to identify the areas for further improvement and implement necessary changes, so it is in line with the overall process.

Based on the monitoring evidences; businesses are required to revise, review and improve at minimum, but not limited to the following while communicating the content to the relevant authorities as mentioned on the core framework:

- Core framework changes
- Risk profile changes
- Target risk profile changes
- Identified risk changes of the pertaining risk scenarios
- Control fine-tuning, replacing or corrective/compensative control implementation
- Update Policies and Procedures

### 2.2.2. Mandatory component

Consist of four main tasks. These tasks ensure the success of the organizational information resilience building process.

1. **Continuous management commitment**

   The management support is continuously required since it gives the necessary leadership and facilitates the information and the resource requirements of the projects, ensuring the overall Information Security and Resilience Framework is a success.

2. **Continuous documentation along with each step**

   Continuous documentation is required though out the process and it will ensure:

   - Formalization
   - Common conduct of the set framework
   - Track record of each step
   - Evidence preservation
   - Ease of monitoring and review
   - Supports the continuity of the process
   - Compliments compliance requirements

3. **Continuous communication with the relevant stakeholders**

   Continuous communication allows companies to be productive and operate effectively. Effective communication will ensure that the information security efforts are better aligned to business and will enable informed, risk aware decision making. This further assists the business to realise the returns on its investments on the information security efforts.

It is of utmost important to ensure information sharing and confidentiality requirements are identified with relevant to internal and external parties and the pertaining risks should come under the identified risks scenarios where the controls should be applied accordingly.

Any communication requirement should be in accordance with the RACI responsibilities defined in the core framework

Continuous communication to the Board/CEO/Owner should take place where the overall progress updates are delivered and the business information security and resilience level decisions are made timely and based on the critical issues arising.

4. **Continuous communication with the foundation layer**

As the core framework provides the necessary guidance to the structure, meaning it shoulders all the efforts of the organization, it needs to be reviewed and adjusted according to the changes that would best supports the organisational goals and objectives. For this, every step of the structure layer process needs to be strictly monitored and communicated to the foundation layer in order for the necessary changes/updates to be reflected up on the core framework.

## 3. How to use the framework

'Information Security and Resilience Framework' will enable the business to manage its information security risks and build its resilience capabilities. The framework assist the business to clearly see across the organizational information security and resilience requirements, while achieving the goals and the benefits mentioned in the introduction of this document.

In order for the business to implement the 'Information Security and Resilience Framework', it requires the business to start by laying the foundation layer. Foundation layer essentially guides the business to establish a business focused, risk based information security governance framework (the "core framework") with its vision to cater to the unique business goals and objectives. It should be assessed and approved by the Board/CEO/Owner before implementation which should set the required tone and importance. Foundation layer has its own cycle: core framework implementation, monitoring and reviewing, which would facilitate continued improvement and review of the core framework according to the business environmental changes. Ensuring the solid foundation is laid, accordingly, the structure layer must be implemented.

An important fact is that this is not a onetime task or a single person event. This requires certain amount of budgets, personnel and support from the entire organisation. Continuous communication and the documentation will further ensure the continuity of the process and enable risk awareness decision making.

The following points are used to create an increased understanding about the framework implementation and how the business may choose to implement. Furthermore, Annexure A will outline steps that would help the business implement the framework as a step-by-step project.

## 3.1. Information Risk Profile

The information security and resilience risk profile of the business is a collection of the risk scenarios analysed to deliver the current threat landscape of the business.

When formulating the risk profile, businesses needs to identify at minimum (but not limited to) the risks pertaining to the business, its internal and external environment, its processes, sub processes, technologies, locations and people, along with the pertaining information, its states (used, transmitted, process, stored), its forms (digital/physical), its legal/compliance requirements, its resilience requirements, who is interested and who has access, and document the gathered information.

## 3.2. Identification of the Risk Scenarios

In order to identify of the risk scenarios, organizations may use the following mechanism.

- First, the business needs to map its information with the processes and the sub processes. There after the processes and the information needs to map with the pertaining: technologies, people and the locations that the information is being used, transmitted, stored and processed; in what form (digital/physical); how it is affected by the nature of the business (internal and external environment); who has access to the information and who are the interested parties to these information; its legal/compliance and resilience requirements. This will give the opportunity to identify most of the possible risk scenarios pertaining to the business information.
- Thereafter, analysing the history of the organisation, similar organisations, local/global information security incidents, understanding the future technologies and the current technologies used globally or by the organizations and their threat landscapes, expert predictions and legal/reputational/compliance issues that would arise based on the business/personal/employee data, resilience requirements and the legal/compliance requirements will further enable to create more risk scenarios that can be of value to the business.

On creating risk scenarios, it is always better to work with different stakeholders, such as (at minimum) legal, finance, risk departments and process owners, who has hands on experience and expertise, will further enrich the threat landscape and facilitate realistic and reliable risk scenarios to be identified which are unique to the business environment.

An important point to note would be that the risk scenarios (RS) needs to have following characteristics: realistic, relevant, impact/loss can be quantifiable (E.g.: High, Low, Medium or in Figures), probability can be defined (E.g.: Probable, Highly Probable, Minor Probability or in Figure) and (if possible) time bounded (When is it expected to occur).

Business may use the following elements to build risk scenarios based on the information gathered.

| Who | Do What | What | Using | When | Impact | Likelihood |
|---|---|---|---|---|---|---|
| Internal with access to information | Intentional Leak | Public | People | Anytime | High | High |
| Internal with no legitimate access to information | Intentional Steal | Internal | Process | Specific | Mediu m | Medium |
| External with access to information | Intentional Destroy | Confidential | Technology | Not Specific | Low | Low |
| External with no legitimate access to information | Intentional Change | | Location | | | |

| | | | | | | |
|---|---|---|---|---|---|---|
| | Intentional Unavailable | | | | | |
| | Unintentional Leak | | | | | |
| | Unintentional Steal | | | | | |
| | Unintentional Destroy | | | | | |
| | Unintentional Change | | | | | |
| | Unintentional Unavailable | | | | | |

## 3.3. Analysis of the Risk Scenarios

For the risk analysis, bank can use quantitative risk analysis models or qualitative risk analysis models based on the data available pertaining to the defined risk scenario. Businesses are required to identify the impacts/losses that the risk scenario will incur (better: for a single occurrence) and the probability/likelihood that the risk scenario will occur (better: annual rate of occurrence).

Impact/Loss (Legal, Reputational, Compliance…etc) needs to be identified, but not limited to the following:

- Impact/Loss incurred to the business due to the risk of confidentiality of the information.
- Impact/Loss incurred to the business due to the risk of integrity of the information.
- Impact/Loss incurred to the business due to the risk of availability of the information.
- Impact/Loss incurred to the availability of the pertaining process.

## 3.4. Selecting Controls to implement/improve

When looking at the controls currently implemented or to be implemented, it is always advised to identify at minimum the following pertaining to the specific risk scenario:

- Proactive control requirements
- Reactive control requirements
- Compliance requirements
- Resilience requirements
- Monitoring requirements based on the set metrics (KPI, KCI and KRI) identified
- Evidence requirements based on the incident handling requirements

With the identification of all the controls available, businesses then need to identify its applicability and the suitability of the control to the business based on the following (but not limited to):

- Estimated cost of the control
- Estimated risk reduction pertaining to the Risk Scenarios (RS)

- Estimated risk reduction pertaining to the other RS
- Estimated Time taken to implement the mechanism
- Suitability to the business (may choose based on the business requirements)
    - Compatibility to the business technologies
    - Appliance/application support availability
    - Appliance/application reliability
    - Third-party service providers reliability
    - Training availability
    - Budget availability
    - Applicable laws, regulations and business maintained standards

Thereafter, the selected controls need to be justified by the pertaining risk/compliance before purchase/implementation. The justification must include, but not limited to: risk, expected benefit and cost.

## 3.5. Setting metrics

By setting up measurable, timely, realistic, informative and actionable metrics, a business could make effective decisions against its information security efforts and enable continuous improvements. Setting up the metrics take place based on two levels.

1. Identify the metrics requirements based on the Risk Scenario (What you require)
2. Identify the metrics capabilities on the controls and technologies (What can be achieved)

Both these metrics should be complimenting each other and necessary fine-tunes should be done according to the suitability and the feasibility to the organization and its goals and objectives.

### 3.5.1. Key Control Indicator (KCI)

Controls are implemented based on the identified risk scenario. Therefore, it should measure the control effectiveness to obtain information on the extent to which a given control is meeting its intended objectives in terms intended risk treatment. Mainly, when developing KCI metrics, the intended risk scenario, its monitoring points and the control/technological capabilities should be understood.

### 3.5.2. Key Risk Indicators (KRI)

KRIs indicates the potential risks that may impact organizational achievements, objectives and decision making. Risk indicators are predictable and are often used as early warning signals, while also tracking trends over a period of time. Considering their importance, it is crucial that they are designed with depth understanding of the business, goals, objectives and its risk profile.

### 3.5.3. Key performance Indicators (KPI)

KPI are developed based on the business goals and objectives while it reflect how well is the organization is performing on achieving its set targets. In terms of information security and resilience, KPI may look at how the organizational information security and resilience goals and objectives are being met at what level.

## 3.6. Monitor, revise, review and improve

As the metrics were decided and set at the Core framework and the Structure Layer-control implementation, the following, (but not limited to) should be monitored:

- Core Framework shall monitor if the set framework is adhered to at the structure layer, is the structure layer introducing new risks to the enterprise risk, and is the structure layer performing as expected.
- Structure Layer will monitor the risk profile and risk appetite of the business, its policies and procedures, control implementation, control operation, control performance, control efficiency on reducing the expected risk.

The gathered monitoring evidences needs to be correlated, analysed and communicated to the relevant personal. Monitoring should be further be able to effectively identify any business environment changes, risk profile changes, processes or new business initiatives that would require business attention.

Based on the final output of the monitoring process, the current policies and procedures must be reviewed/revised to reflect any changes/updates/improvements required and where the current policies and procedures does not address, it should be added as a new policy/procedure or in to the existing to ensure that the process is always in the correct path that allows the business to achieve its goals and objectives. This should take place regularly on a reasonable time period basis and whenever there is a policy/procedure change required urgently.

## 3.7. Analyzing the controls effectiveness and efficiency

With proper metrics and the monitoring in place to identify how the control is performing against the pertaining risk scenarios, businesses can clearly identify if the implemented controls incurs a loss or a benefit to the business.

Moreover effective metrics and the monitoring could easily identifies if the controls needs to be fine-tuned, replaced or does it need to add more compensative or corrective controls.

Further, business needs to identify if the control assist or enhances the entire process and does the control enable the business capabilities to achieve its goals and objectives or if it disrupts.

This should be performed regularly and take necessary actions to get better advantage and ROI from the controls.

## 3.8. Adding value to the business

By applying risk based controls in to the process where it secures and enrich the operation, it can also bring to the business more value addition to gain customer trust and business advantages.

## 3.9. Building a risk aware culture

When human is the weakest link in information security and the hardest to manage, best way possible is to develop a risk aware culture. It is the culture where all the employees in the organization are capable of clearly identifying risks and has a knowledge on detecting any abnormalities take place, and communicate to the relevant parties. Risk aware culture is developed with the leadership and commitment of the executives and the top management by adopting and following the information security policies and procedures. This is then absorbed in to the daily routines, rituals, and behaviours of the company. Developing a risk aware culture takes time and efforts as well as the management commitment.

# 4. Annexure A - Suggested Steps on framework implementation

Suggested guidelines of the Framework Implementation are spelt out below. Business may use the same or combine it with their own version to implement the framework.

| **Foundation Layer** |
|---|
| **Implementing the CORE framework** |
| • Appoint a CISO/C-Level person in charge of overall information security |
| • Issue a board level support statement for the framework |
| • Define overall framework roles and responsibilities |
| • Define overall framework matrices to oversee the performance and risks |
| • Define overall framework monitoring mechanisms and timelines |
| • Define overall framework governing policy and procedures |
| |
| **Structure Layer** |
| **Formulating the Risk Profile** |
| • Create Risk Scenarios |
| ○ Background Work |
| ▪ Understand the business, its Internal and the External Environment |
| ▪ Identify the business goals and objectives |
| ▪ Identify the Processes |
| ▪ Identify the sub processes |
| ▪ Identify the technologies |
| ▪ Identify the people |
| ▪ Identify the locations |
| ▪ Identify who has access to the business data/information |
| ▪ Identify who are the interested parties of the business data/information |
| ▪ Identify the Legal and Regulatory/Compliance requirements |
| ▪ Identify the information resilience requirements to meet business resilience requirements |
| ▪ Identify the data/information available for the business |
| ▪ Identify the information states (use, process, transmit and store) and forms (physical/digital) |
| ▪ Map the information, states and forms with all the information gathered |
| ○ Identify the Risk Scenarios |
| ▪ Locate each point in the map and identify what could affect negatively the business goals and objectives (Risk Scenarios - RS). Business could use the following aspect to create realistic and relevant RS: |
| → Who |
| → Do What |
| → What |
| → Using |
| → When |
| ▪ Identify the Impact and the Likelihood of each RS. E.g.: |
| → Impact/Loss incurred to the business due to the risk of confidentiality of the information |
| → Impact/Loss incurred to the business due to the risk of integrity of the information |

| |
|---|
| → Impact/Loss incurred to the business due to the risk of availability of the information |
| → Impact/Loss incurred to the availability of the pertaining process |
| ▪ Identify the criticality of the specific process/data to the business |
| • Prioritise RS |
| o Prioritise the RS based on (at minimum): |
| → Criticality of the specific process/data to the business |
| → Impact that the Risk Scenario may cause |
| → Likelihood of the Risk Scenario |
| → Time expected to occur of the risk scenario |
| **Identification of the target risk profile** |
| • Identify the risk acceptance levels to each RS identified (Business may choose to decide for individual or similar groups of risk scenarios) |
| **Identification of the risk treatment techniques and controls to bridge the gap** |
| • Identify the gap between the Current and the Target Risk Profile |
| • Identify the risk treatment techniques available for reducing each gap |
| • Identify the treatment categories and options available under each treatment techniques |
| • Identify the controls available under each category/option. Controls need to be identified at minimum looking in to the following areas: |
| → Proactive requirements |
| → Reactive requirements |
| → Compliance requirements |
| → Resilience requirements |
| → Monitoring requirements based on the set metrics (KPI, KCI and KRI) identified |
| → Evidence requirements based on the incident handling requirements |
| • Analyze the controls to gain an understanding the applicability and the suitability of the control to the business. Following are areas (at minimum) should be looked at: |
| → Estimated cost of the control |
| → Estimated risk reduction pertaining to the Risk Scenarios (RS) |
| → Estimated risk reduction pertaining to the affiliated RS |
| → Estimated Time taken to implement the mechanism |
| → Suitability to the business (may choose based on the business requirements) |
| ❖ Compatibility to the business technologies |
| ❖ Appliance/application support availability |
| ❖ Appliance/application reliability |
| ❖ Vendor reliability |
| ❖ Training availability |
| ❖ Budget availability |
| ❖ Applicable laws and regulations |
| ❖ Business compliance to standards and best practices (E.g. ISO, NIST, SANS, CIS…etc) |
| • Prioritise the risk treatment techniques, categories/options and controls based on the business requirements (E.g.: Lowest cost, better applicability and higher risk reduction can be first…etc.) |
| **Planning and Implementation** |
| • Create long term and short term plans to implement |
| • Create business case per control stating at minimum (but not limited to) the risk, expected benefit and cost and get approved by the relevant personal as stated on the core framework |
| • Define metrics per control |

| |
|---|
| • Define policies and procedures per control |
| • Implement according to the policies and procedures |
| • Communicate and update the policies/procedures and metrics if any changes/updates required |
| **Continuous monitoring and reporting** |
| • Monitor the overall risk profile changes |
| • Monitor the overall target risk profile changes |
| • Monitor the implemented controls according to the metrics defined |
| • Report to the relevant parties to make informed-risk aware decision making |
| **Continuous revise, review and improvement** |
| • Business needs to revise, review and improve at minimum, but not limited to the following |
| → Core framework changes |
| → Risk profile changes |
| → Target risk profile changes |
| → Identified risk changes of the pertaining risk scenarios |
| → Control fine-tuning, replacing or corrective/compensative control implementation |
| → Update Policies and Procedures |

# 5. Annexure B : Definitions

This appendix defines selected terms used in the framework.

| | | |
|---|---|---|
| Information Security | : | Safeguarding (but not limited to) confidentiality, integrity and availability (CIA) of the information and its related systems from unauthorized access, use, misuse, disclosure, disruption, modification, or destruction |
| Information Security Risk | : | Information security risk is chance or possibility of an security event affecting an organization's confidential information |
| CIA Triad | : | CIA triad is (Confidentiality, integrity and availability) model designed to guide policies for information security within organization. |
| Information Resilience | : | Business's ability to withstand and quickly recover from possible information security threats that disrupts it from achieving its goals and objectives |
| Risk Scenarios | : | Risk scenario is potential incident that can occur within the organization. |
| Business Risk Appetite | : | Business risk appetite is amount and type of risk that organization is willing to take in order to pursuit of business organization |
| Risk Treatment | : | Risk treatment is range of strategies used to reduce the risk |
| Controls | : | Controls are specific activities follow to reduce an identified risk |
| Risk Registry | : | Risk register is document that contain possible risk and action to manage each risk |
| Key Performance Indicators | : | Key performance indicator is when organization define its performance targets based on its goal and objectives and monitor its progress toward goals. |
| Key Risk Indicators | : | Key risk indicator is used to measures the company's level of risk by define its risk profile and monitor changes in that profile. |
| Key Control Indicators | : | Key control indicator Indicates how effectively internal controls are working. |
| Risk Profile | : | Risk profile is type of threats an organization face currently. |
| Target Risk Profile | : | Acceptable level of risk pertaining to the risk scenario identified organization is willing to take in order to achieve its business goals and objectives |

# 6. Annexure C : Acronyms

This appendix defines selected acronyms used in the framework.

| | | |
|---|---|---|
| RACI | : | "Responsibility, Accountability, whom to Consult and who to Inform" |
| ROI | : | Return Of Investment |
| KPI | : | Key Performance Indicator |
| KRI | : | Key Risk Indicator |
| KCI | : | Key Control Indicator |
| RS | : | Risk Scenario |
| CIA Triad | : | Confidentiality, Integrity and Availability |