# Revision History

| Date | Version | Description | Author | Reviewer |
|---|---|---|---|---|
| 19/05/2015 | 1.0 | Issue version | | |
| 23/07/2019 | 2.0 | Generalization for company use and for ISO 27001 | | |
| 19/04/2021 | 3.0 | 3rd issue version | | |
| 02/06/2022 | 4.0 | 4th issue version, minor change related requirements of the certificate | | |
| 28/05/2024 | 5.0 | - Updated according to the requirements of ISO 27001:2022 Standard<br>- Updated according to 's Information Security Policies and Information Security Risk Management Framework<br>- Update security label based on ’s CS-ST-06-Information Classification and Handling Standard<br>- Update Company’s logo | | |

# Table of Contents

# List of Tables and Figures

# 1. INTRODUCTION

## 1.1 DEFINITIONS, ACRONYMS AND ABBREVIATIONS

*Risk Manager:* Role responsible for driving the risk assessments and applying the risk management framework to obtain adequate results. They coordinate with the relevant roles and positions for the progress of the assessments and register the results and present them to the relevant instances. They conduct the monitoring and follow up of risks.

*Risk Owner:* Role designated to the person or area accountable for the process or asset being assessed. They are responsible for managing the risks identified in their scope of action and provide, as subject matter experts, any information relevant for the analysis.

*Risk Approver:* Role played by a person or area in position to determine the adequacy of a treatment plan over a given risk and to approve or disapprove its effectiveness to reduce the inherent risk.

| No | Abbreviations | Description |
|---|---|---|
| 1. | **N/A** | Not Applicable |
| 2. | **CEO** | Chief Executive Officer |
| 3. | | Chief Information Security Officer |
| 4. | **The Company** | |

Table 1.1 – Definitions, Acronyms, and Abbreviations

## 1.2 PURPOSE

This document describes the risk management process. This is the common framework for XXX-XXX in the different dimensions of Risk Management, especially Security Risk Management to ensure the proper administration and acceptable level of risks, to maintain the security of internal operations as well of the delivery of services to clients.

## 1.3 SCOPE

This process shall be applied to any process or planned activity within The Company.

## 1.4 REFERENCES

| No | Document | Code | Description |
|---|---|---|---|
| 1. | 's Information Security Policies and Standards | N/A | Current 's Information Security Policies and Standards |
| 2. | _Sổ tay An toàn thông tin | ISMS/CS_SAT001 | Information Security Manual of |
| 3. | ISO 9001:2015 Quality Management Systems — Requirements | EN ISO 9001:2015 | Requirements of Quality Management System,<br>International Organization for Standardization |

| | | | |
|---|---|---|---|
| 4. | ISO 27001:2022 Information technology — Security techniques — Information security management systems — Requirements | EN ISO 27001:2022 | Requirements of Information Security Management System,<br>International Organization for Standardization |
| 5. | Quality Manual | QMS/PL_QMN001 | Quality Manual of the ’s QMS |
| 6. | Risk register template | ISMS/PR_RSK001/T001 | |

Table 1.2 – References

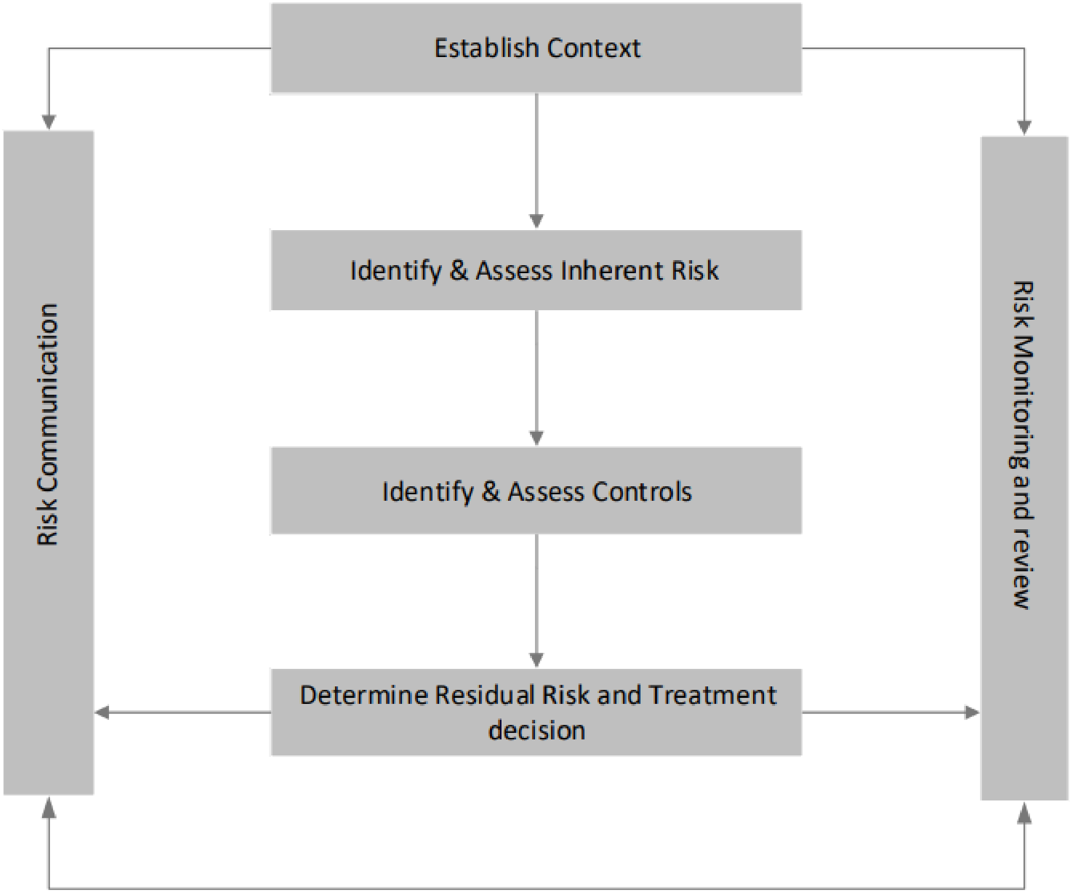
# 2. PROCESS

## 2.1 PROCESS CHARACTERISTICS

| Characteristic | Description | Requirements |
|---|---|---|
| Involved workers | • Board of Director<br>•<br>• Head of Unit<br>• IT<br>• Manager/Team leader<br>• All employees | • Preliminarily introduction to risk management |
| Entry criteria | • Before deploying any planned activity, such as a project, hardware procurement, network planning and installation, environment change, or on request.<br>• In considering contract with customer having information security responsibilities of<br>• At least once a year or when there are major changes in the Company's context, information assets as well as changes in the requirements of related, the previously accepted risks must be reassessed to update the risk-related changes in the current context and determine the next handling plan | • Activity plan or schedule must be available. |
| Exit criteria | • Risk register with risk treatment plans | • N/A |
| Metrics | • Risk occurrence rate = Number of risks that occur / Total number of listed risks | • Risk occurrence rate < 30% |
| Related processes | • N/A | • N/A |
| Tools | • N/A | • N/A |

Table 2.1 – Process characteristics

## 2.2 WORKFLOW



Establish Context
Risk Communication
Identify & Assess Inherent Risk
Identify & Assess Controls
Determine Residual Risk and Treatment decision
Risk Monitoring and review

2.1 – Process workflow

## 2.3 ACTIVITIES

### 2.3.1 ESTABLISH THE CONTEXT

Every Assessment must begin by confirming the current context in which it is being carried on. This background must be comprised of the relevant circumstances, both internal and external to the company:

- Description of process or asset that's being assessed and its contribution in the overall business operations of the company. Person or area responsible for its management. Internal dependencies relevant to its proper functioning. Determine the relevant internal stakeholders that must be involved in the assessment.
- Requirements defined by Top Management (e.g., new legal, regulatory, or contractual requirements applicable to XXXXXXX, new services, new infrastructure, new relations with external entities).
- Information obtained in previous iterations of the Risk Management process.
- Identify known or suspected threats the process or asset may be subject to (can be detected in periodic monitoring activities or through information obtained externally to XXXXXXX).
- Information obtained through regular meetings with the heads of the business support teams (Office, HR, Legal, IT Infrastructures and Procurement), as well as the heads of the XXX Corporate Security Teams.

### 2.3.2 IDENTIFY AND ASSESS INHERENT RISKS

#### 2.3.2.1 Identify Inherent Risks

Risk identification is carried out on any set of tasks and its objective is to determine which events may have a potential impact on XXXXXXX and to gain knowledge about how, when, and why this impact may occur. The identification of information security risks should ensure alignment with business objectives and not focus solely on purely technological aspects. To this end, risks should be reflected in business impact and, in this sense, threats affecting each asset under analysis should be framed in the following set of business attributes:

- Confidentiality - ensuring that information is not available, accessible or disclosed to unauthorized individuals, entities or processes.
- Integrity - to ensure that the information is protected against corruption or unauthorized modification. Availability - to ensure that the information is accessible and usable whenever requested by an authorized entity.
- Traceability - to ensure that the actions of an entity can be attributed exclusively to that entity. Authenticity - to ensure that an entity is who it claims to be or that it guarantees the source of the data.

The tasks that constitute this activity are:

**Asset identification**

It will be up to the team involved in this activity to define the scope of the assets to be considered, depending on the objectives initially defined and the deadline for carrying out the iteration. The definition of assets must be carried out with an adequate level of detail so that sufficient information is provided for the evaluation of information security risks. The information to be collected in this task typically falls into the following categories:

- Business processes involving assets.
- Owners, users, and asset support teams.
- Type, criticality, and sensitivity of information.
- Asset location and function.
- Support infrastructure (e.g., network, security).
- Requirements (e.g., legal, regulatory, XXX-XXX-XXX policies and regulations).

**Threats and vulnerabilities identification**

To identify the likelihood and impact of the risks to which identified information assets are exposed, threats and potential vulnerabilities must be considered:

- Threat - Potential cause of an unwanted incident, which can exploit a vulnerability to damage assets such as information, processes, and systems and therefore XXX-XXX-XXX . Threats can be of natural origin and can be accidental or deliberate and can arise from the XXX-XXX-XXX internal or external environment.
- Vulnerability - A failure or weakness in procedures, design, implementation, operation, or internal control, which may result in an Information Security breach or violation of rules defined in Information Security regulations.

This task aims at identifying possible information security threats and their sources, considering the following aspects:

- Threats should be identified generically and by type (e.g., unauthorized actions, physical harm, technical failures) and therefore, where appropriate, individual threats should be identified within a generic class.
- Some threats may affect more than one asset. In some cases, they may cause different impacts depending on the assets that are affected.
- Information can be obtained by reviewing incidents, gathering from XXX-XXX-XXX elements (e.g., asset owners, users, technical teams) and analysing other sources, including external threat catalogues.
- Relevant threats are constantly evolving, especially if the business environment or information systems change.

As a result of performing this task, a list of threats that can be exploited by vulnerabilities, associated with each asset under analysis, is obtained.

**Controls identification**

This task aims at identifying information security controls (existing or planned) that aim to ensure a reduction in the level of risk of assets. The identification should be carried out based on existing documentation, implementation plans and meetings with technical areas and should be identified:

- Existing controls - existing controls should be identified and an assessment of their state of implementation should be made to ensure their proper functioning and adequacy. The effect of implementing a control can be estimated by gauging how it reduces the likelihood of the threat and the ease of exploiting the vulnerability or the impact of the incident.
- Planned controls - controls in the process of implementation should be identified or defined for the near future in planning.

#### 2.3.2.2 Assess Inherent Risks

The main objective of this activity is to classify the level of inherent risk based on the probability and consequence of the threat's achievement.

Inherent Risks assessment should consider how often threats are realized and how easily vulnerabilities can be exploited, considering factors such as:

- Experience and statistics applicable to the probability of threats.
- Sources of deliberate threats: the motivation and capabilities, which change over time, and resources available to possible attacks, as well as the perception of asset vulnerability.
- Sources of accidental threats: geographical factors such as occurrence of extreme weather conditions and other factors that may influence human error and equipment malfunction.
- Vulnerabilities, individually or in aggregate.
- Existing controls and how to effectively reduce vulnerabilities.
- Concerns of stakeholders.

The analysis of the level of risk is based on a two-dimensional analysis Impact and Likelihood:

**Impact (Identification of consequences)**

The assessment made for any given risk must have the most objective approach to the foreseeable impact it could make in the event of materializing, based on the Asset or Process owner’s and the Risk Manager’s knowledge and experience, as well as a critical analysis of the sector.

The impact must be based on at least one of the following categories. In the event that more than one category is assessed, the level of impact will be based on the one with the highest value.

The following describes the levels of impact of a risk occurring:

| Impact Level | Economic results | Operations | Reputation | Compliance | Safety of employees |
|---|---|---|---|---|---|
| **VERY HIGH** | The potential damage caused by the event may be more than 20% of yearly operating income | Business continuity is endangered. Very negative impact on the achievement of Company objectives. Long interruption of key processes. Very | Very high potential impact on corporate image and reputation in both national and international arena | Potentially high fines and prosecution of employees and managers. Interruption of operations ordered by Authorities | Employees’ death and serious illness/injury impact (mass retirement, occupational health and safety issues) is critical at |

| | | | | | |
|---|---|---|---|---|---|
| | | relevant loss of quality of services | | | level. |
| **SIGNIFICANT** | The potential damage caused by the event may be between 12% and 19% of yearly operating income | 5 or 6 operating processes are affected. Negative impact on the achievement of Company objectives. Interruption for some key processes. Relevant loss of quality of services | High potential impact on corporate image and reputation in both national and international arena | Possible high fines. Restriction on operations ordered by Authorities | Employee's illness/ injury impact (retirement of key personnel, occupational health and safety) is critical on specific departments but also some impact at level. |
| **MEDIUM** | The potential damage caused by the event may be between 8% and 12% of yearly operating income | 3 or 4 operating processes are affected. Medium impact on the achievement of Company objectives. Short interruption for some key processes. Moderate loss of quality of services | Moderate potential impact on corporate image and reputation in national context (e.g., news reported in national media in more than one country) | Medium fines. Frequent relevant sanctions by Authorities. Massive complaints by customers. Serious disputes with competitors. Relevant sanctions arising from ongoing proceedings with Authorities | Employee's serious illness/ injury impact (retirement of key personnel, occupational health and safety) is Critical on specific departments |
| **LOW** | The potential damage caused by the event may be between 2% and 8% of yearly operating income | 1 or 2 operating processes are affected. Low impact on the achievement of Company objectives. Short interruption for some key processes. Low loss of quality of services | Low potential impact on corporate image and reputation in national context (e.g., news related to a legal entity reported in local media) | Possible minor fines. Frequent minor sanctions by Authorities. Frequent complaints by customers. Disputes with competitors. Start of inspections by Authorities | Damage or negative impact on specific employees. |
| **NEGLIGIBLE** | The potential damage caused by the event may reach up to 2% of yearly operating income | Negligible impact on achievement of Company objectives and on quality of services | Negligible potential impact on corporate image and reputation of Group | Possible fines of negligible value. Occasional minor sanctions by Authorities. Occasional complaints by customers | No employee is harmed or injured. |

Table 2.2 – Impact

**Likelihood**

The following describes the levels of likelihood of a risk occurring, with analysis of Forecast, Statistic and Measurability:

| Likelihood | Forecast | Statistic | Measurability |
|---|---|---|---|
| **VERY HIGH** | The event will probably occur in the short term, frequently next year | The event occurred at least once every year in the past five years | The event occurs in more than 50% of cases |
| **HIGH** | The event will probably occur in the short term, sometimes next year | The event occurred at least once every year in the past three years | The event occurs in between 20% and 50% of cases |
| **MEDIUM** | The event will probably occur in the medium term, sometimes in the next five years | The event occurred at least once in the past three years | The event occurs in between 5% and 20% of case |
| **LOW** | The event will probably occur in the long-term (in more than five years) | The event occurred at least once in the past five years | The event occurs in between 1% and 5% of cases |
| **REMOTE** | The event will probably not occur in the long-term (five years or more) | The event occurred at least once in the past five years | The event occurs in less than 1% of cases |

Table 2.3 – Likelihood

The value for impact and probability will be the highest applicable when considering each driver in each section. For instance, if compliance impact for an event is "HIGH", while other impacts are either lower or not applicable, the impact level for that event will be "HIGH". Both impact and probability shall be evaluated in a "what if" scenario, i.e not considering existing countermeasures. Risk of fire (its impact and probability) should not be considered a smoke detection system in place, as well as risk of cyber-attack should be assessed without taking into account the effectiveness of the information security system in place.

Probability is valued considering known past events (as absolute numbers or as percentage of cases), and chances that the event will occur in the foreseeable future (short/medium/long term).

Forecast: This evaluation gives an estimate of an event occurrence in the future.

**Level of risk**

Once the levels of Likelihood and Impact are stablished, the resulting risk level is automatically set within following the Risk Matrix, resulting in the final level of risk.

## Risk Matrix

| Likelihood | | | | | |
|---|---|---|---|---|---|
| VERY HIGH | LOW | MEDIUM | HIGH | VERY HIGH | VERY HIGH |
| HIGH | INSIGNIFICANT | MEDIUM | HIGH | VERY HIGH | VERY HIGH |
| MEDIUM | INSIGNIFICANT | LOW | HIGH | HIGH | VERY HIGH |
| LOW | INSIGNIFICANT | LOW | MEDIUM | MEDIUM | HIGH |
| REMOTE | INSIGNIFICANT | INSIGNIFICANT | LOW | LOW | MEDIUM |
| | NEGLIGIBLE | LOW | MEDIUM | SIGNIFICANT | VERY HIGH |
| | Impact | | | | |

Table 2.4 – Risk Level

### 2.3.3 IDENTIFY AND ASSESS CONTROLS

Controls associated to the identified risks must be assessed individually on their maturity and operational efficiency and as a whole, to determine their risk reduction capability.

The final appreciation of risk reduction should consider the various possible controls on a single risk altogether referred to as "Control in place" - Level of control for the risk.

| Control in place | Definition | Reduction |
|---|---|---|
| **NOT EFFECTIVE** | Control in place to prevent the risk, detect events and/or mitigate its effects are not in place or they have revealed not effective in design and implementation. | There is no reduction between inherent and residual risk score. |
| **PARTIALLY EFFECTIVE** | Procedures are applied to mitigate the risks but there is lack or poor evidence of a formalized process, of clear appointment of roles and responsibilities, of establishment and monitoring of KPI. | There is a reduction between the inherent and residual risk score. |
| **EFFECTIVE** | Governance, Key Risk Indicators (KRI) and countermeasures are formalized, in place and effective. Governance: process and procedure for risk control are in place and formalized; KRI | There is a significant reduction between the inherent and residual risk score. |

| | | |
|---|---|---|
| | to assess risk thresholds and/or alerts are set and monitored; countermeasures: procedures and actions are in place aiming to handle prevention, detection of events and mitigation of impacts. | |

Table 2.5 – Level of control for the risk

### 2.3.4 DETERMINE RESIDUAL RISK AND TREATMENT DECISION

#### 2.3.4.1 Residual Risk

Residual risk is the result of the adjustment of the assessed inherent risk being modified by the strength of controls.

Criteria for the reduction of risk:

- Controls may reduce Probability, Impact or both. Residual risk is obtained from the new values.
- Numerous controls are no guarantee of a significant reduction in risk.
- Inherent Very High Risks may not be lowered more than Medium Residual Risk level.

The following describes the analysis to determine the level of reduction provided by control measures:

| **Likelihood** | | **Impact** | | **Inherent/Residual Risk** | | **Control in place** | |
|---|---|---|---|---|---|---|---|
| **Level** | **Score** | **Level** | **Score** | **Level** | **Score** | **Level** | **Score** |
| REMOTE | 1 | NEGLIGIBLE | 1 | INSIGNIFICANT | <=4 | NOT EFFECTIVE | 1 |
| LOW | 2 | LOW | 3 | LOW | >4 | PARTIALLY EFFECTIVE | 0.7 |
| MEDIUM | 3 | MEDIUM | 7 | MEDIUM | >10 | EFFECTIVE | 0.2 |
| HIGH | 4 | SIGNIFICANT | 10 | HIGH | >20 | | |
| VERY HIGH | 5 | VERY HIGH | 12 | VERY HIGH | >35 | | |

Table 2.6 – Level of reduction risk

The Risk Value is obtained based on the following formula:

Inherent Risk Value = Likelihood x Impact

Residual Risk Value = Inherent Risk Value x Level of control for the risk (Control in place)

#### 2.3.4.2 Treatment Decision

**Risk Appetite**

The risk appetite is the amount of risk the organization is willing to pursue or accept. It is set by the Risk Governing Bodies at XXX level.

The residual risk level must be contrasted with the current risk appetite in order to determine the actions to take regarding any given risk.

**Accept/Tolerate**

The residual risk is considered acceptable by the roles driving the risk assessment. Meaning that the consequences of it materializing can be absorbed and don’t reasonably pose a threat to the overall objectives of the organization.

For risks below the organisation’s risk appetite, the acceptance of the risk owner and approver is considered enough.

For risks above the organisation's risk appetite, a formal request for acceptance is required from the risk governing bodies at XXX level.

**Treat/Mitigate**

The residual risk is not acceptable, and it is deemed necessary to reduce it by means of one or more treatment measures, which could be implemented internally or by another area.

These treatment measures must be formally stated and monitored in the risk register to guarantee the desired result of decreasing the residual risk levels.

Initiatives or projects that address risks of special relevance to the organization, must receive special attention and be periodically reported on their progress to the top management.

**Transfer**

The residual risk is considered a liability, and it is deemed necessary to have a guarantee that, in the event of it materializing, the organization is reasonably covered.

Contractual agreements with third parties, such as insurance companies or outsourcers, must be signed, specifying the level of responsibility each actor has in the event of the risk materializing.

The decision to transfer the risks must be driven by the Risk Owner and informed or raised for decision by the relevant stakeholders, depending on the strategic relevance of the activity.

**Avoid/Terminate**

The residual risk is considered unacceptable, and the costs of trying to reduce it or transferring it are not reasonable or worth the effort. Therefore, the asset or process that generates the risk must be terminated.

The scenario to terminate any given activity due to the level of risk must be thoroughly analysed for impacts on the overall objectives of the organization and raised for decision to the relevant instances.

Although these considerations may affect the decision, considering the level of risk obtained in the "Determine residual risk" activity, measures should be implemented for risks with a "Very High" or "High" level, as defined in the following table:

| Risk | Action | Prioritization criteria |
|---|---|---|
| **VERY HIGH** | The risk cannot be accepted. It must be prioritized and treated within 3 months. | 1 |
| **HIGH** | The risk cannot be accepted. It must be prioritized and treated within a | 2 |

| | | |
|---|---|---|
| | year. | |
| **MEDIUM** | The risk can be accepted but should be closely monitored (it might need the implementation of monitoring measures). | 3 |
| **LOW** | The risk can be accepted. | 4 |
| **INSIGNIFICANT** | The risk can be accepted. | 5 |

Table 2.7 – Actions to be taken according to the Level of Risk

### 2.3.5 COMMUNICATION, MONITORING AND REVIEW

During the analysis, stakeholders must be kept informed of its progress, with an emphasis on communicating the results at the end of the iteration.

The results of each assessment must be logged into a risk register to facilitate the monitoring of the proposed actions and the effect they have on the criticality of the risks found.

The risk management cycle must be carried out periodically, with annual repetitions as a standard, and when significant changes occur that affect the context of the organization.

## 2.4 RISK APPROACHES

There are different approaches to risk management, depending on the nature of the process being assessed, the regional scope or the type of assessment.

Valid risk approaches include:

- **Asset based**: Focused on the security of specific, or logically aggregated, IT assets that are relevant for operations.
- **Business based**: Directed at assessing the procedural, technical and compliance security risks that may affect specific business projects or products that are delivered to clients.
- **Operational**: Directed at assessing all the possible risks that may affect business objectives set out by the company, and its operations.