Purpose

The purpose of this policy is to establish a formalized procedure for Risk Assessment Process in terms of information assets and information resources.

Scope

This policy applies to all employees, contractors, subcontractors, consultants, temporaries, guests, and any third party that uses information assets or information resources and services.

Responsibilities

This Risk Assessment provides provisions for all service activities and the information technology system required to operate those activities. Responsible persons for this procedure are

CEO:

Lead the reviewing of the Risk Assessment spreadsheet at a minimum annually.

Maintain copies of annual Risk Assessment documents for 3 years.

ISMS Manager:

■ollect all information related to critical assets and company processes.

Perform the Risk Assessment at a minimum annually.

Risk Owners:

Maintain the critical assets or company processes.

Approve the risks and risk scores associated with their processes and assets with ISMS Manager.

Carry out the risk treatment process associated with their asset or process with ISMS Manager.

Policy

Annual Review of Risk Assessment

should conduct an annual, formal Risk Assessment that identifies current and possible risks and vulnerabilities. Also, should review its policies, procedures, standards, and guidelines following the updated Risk Assessment and make any applicable modifications to counter evolving threats.

Risk Assessment Procedure

Risk Assessment is a proactive process by which:

Hazards are identified;

The risks associated with the hazard are evaluated;

Appropriate methods to eliminate or control the hazard evaluated.

Step 1 – Identify the hazard:

Look at your critical infrastructure and systems that you use (Critical Asset Registry).

Talk with responsible persons across the company.

Analyze recent accidents/incidents.

Step 2 – Decide who may be harmed and how:

Include the employees, contractors, customers, new and expectant ones.

Step 3 – Evaluate the risks:

Check what controls are in place.

Decide if the risk is acceptable/avoidable/needs to be transferred or mitigated.

Are further precautions required to eliminate or reduce the risk further?

Prioritize the actions by their risk score.

Step 4 – Record your findings and implement them:

Record assessment in Risk Assessment.

Risk Assessment Structure

General Risk Information

Risk No. - Risk number.

Type of risk:

Operational risk occurs in case of inadequate or failed procedures, systems, or policies.

Documentation risk occurs in case of unforeseen events with legal/financial/contractual documentation.

Compliance risk occurs when the company fails to comply with industry laws and regulations, internal policies, or prescribed best practices.

Reporting risk occurs when fails to correctly report statements.

Legal risk occurs when there are some sort of internal problems that lead to legal problems.

General risk category - general description of risks.

Detailed risk scenarios - description of possible risk events that will have an uncertain negative impact on achieving business and ISMS goals.

Risk owner - is an accountable person, who coordinates efforts to manage the risk.

Assets associated with risks - asset name.

Type of Asset - the category of our assets:

People;

Documentation;

Equipment for Physical Security;

Software;

Hardware;

Virtual Machine Data Storage;

Network Infrastructure;

Operational Data;

Communication;

Office;

AWS service.

Asset owner - is the person responsible for the day-to-day management of assets.

Risk Management

Existing controls, policies, procedures, or processes - description of all actions that already exist in .

Likelihood - the probability of the risk occurring.

1 - Rare;

2 - Unlikely;

3 - Moderate;

4 - Likely;

5 - Almost Certain.

Impact - the estimate of the potential losses associated with an identified risk.

1 - Very Low;

2 - Low;

3 - Medium;

4 - High;

5 - Very High.

Existing risk rating - done by multiplying Impact Score and Likelihood, an estimate of the potential losses associated with an identified risk.

1 - Very Low;

2 - Low;

3 - Medium;

4 - High;

5 - Very High.

Further risk treatment (YES/NO) - the decision if the risk should be treated.

Approval tab - the tab where the risk owner puts “Approved” if he/she acknowledges the importance and the relevance of this risk, and agrees with the given risk score.

Risk Treatment

Vulnerabilities associated with risk - gaps or weaknesses that create risks.

Proposed mitigation actions - specific actions taken to reduce or eliminate risk, or to exclude weaknesses.

Mapped ISO/IEC 27001 Annex A ■ontrols - ISO/IEC 27001 list of controls that a business is expected to review for applicability and implementation.

Actual likelihood - the probability of the risk occurring.

1 - Rare;

2 - Unlikely;

3 - Moderate;

4 - Likely;

5 - Almost Certain.

Actual impact - the estimate of the potential losses associated with an identified risk.

1 - Very Low;

2 - Low;

3 - Medium;

4 - High;

5 - Very High.

Actual risk rating - done by multiplying Impact Score and Likelihood, an estimate of the potential losses associated with an identified risk.

1 - Very Low;

2 - Low;

3 - Medium;

4 - High;

5 - Very High.

Current control effectiveness - a relative assessment of the actual level of control that is currently present and effective, compared with that which is reasonably achievable for a particular risk.

Non-existent;

Poor;

Fair;

Good;

Very Good.

Status:

TO DO;

IN PROGRESS;

DONE.

Responsibility - who is responsible for this risk and all actions related to that and will perform a risk treatment plan.

Step 5 – Review Assessment

Assessments should be reviewed every year, or earlier if it is suspected that the assessment is no longer valid.

Risk Assessment Procedure before a new project

All risks for current services () are evaluated in the Risk Assessment. So, most of the risks regarding these projects are covered there, but still the Assessment should take place to find the particular risks.