

Table of Contents

1. Introduction.....	3
2. Purpose	3
3. Scope.....	3
4. Terms and Definitions	3
5. Compliance Table	4
6. Review	4
7. ISMS Risk Statement.....	4
8. Frequency of Risk Assessments	5
9. Responsibility and Authority.....	5
9.1 Management.....	5
9.2 Responsibility Matrix	6
10. Risk Assessment Methodology.....	7
10.1 Asset Identification and Classification.....	7
10.2 Grouping of Assets	9
10.3 Identification of Threats and Vulnerabilities	9
10.4 Assessment of Threats	9
10.5 Assessment of Vulnerability	10
10.6 Calculation of Risk Rating.....	11
10.7 Identify Risks	12
10.8 Identify Risk Owner	12
10.9 Acceptable Risk	12
10.10 Risk Treatment and Management.....	13

DOCUMENT CONTROL

VERSION CONTROL

Document Control ID	EFR-Risk Management Procedure-035
Issued Date	
Effective Date	
Owner	Information Security & Compliance Department

REVISION TABLE

Date	Version	Brief Description	Author

RELEASE AUTHORIZATION

Task	Author	Title	Date

REVIEWER AUTHORIZATION

Task	Author	Title	Date

APPROVAL AUTHORIZATION

Name	Title	Signature	Date

Important Note: This document is intended solely for the use of the individual or entity to whom it is transmitted to and others authorized to receive it. It may contain confidential or legally privileged information. If you are not the intended recipient you are hereby notified that any disclosure, copying, distribution or taking any action in reliance on the contents of this document is strictly prohibited and may be unlawful. If you have received this document in error, please notify us immediately.

1. Introduction

The Risk management procedure outlines the risk assessment methodology and provides guidance to identify relevant risks further, it also outlines the frequency to perform the risk assessment. This risk assessment procedure is applicable specifically to ISMS and not to other areas of the organization.

2. Purpose

The purpose of risk management is to identify potential problems before they occur so that risk-handling activities may be planned and invoked as needed across the life of the product or project to mitigate adverse impacts on achieving objectives.

3. Scope

The document details the procedure through which the organization shall identify and handle the risks it might be exposed to within the realm of its Information Security Management Systems (ISMS). It also provides clarity on responsibilities and accountabilities for the various participants in the overall management of risk in the organization. It encompasses the following areas:

- Criteria for performing risk assessment and frequency of risk assessment.
- Responsibility and authority.
- Identifying the assets and their related risks within ISMS and the applicable threats, vulnerabilities and existing controls.
- Estimating the impact and probability of threat and vulnerability.
- Identify the risk owner.
- Evaluating the risks against risk acceptance criteria.
- Determining how risks should be treated and criteria for accepting identified risks.
- Obtain risk owner approval on risk treatment plan and acceptance of the residual risk.
- Outlining how risk decisions should be communicated.
- Maintaining the monitoring and reviewing of information security risks.

4. Terms and Definitions

Risk management definitions for the purposes of the organization's ISMS are designed by leveraging industry reference standards such as AS/NZS 4360:1999 - Risk Management, BS 7799-3 Guidelines for Information Security Risk Management, NIST SP800-30 Risk Management Guide for Information Technology Systems, ISO 27005/ISO 31000, etc. The key definitions for this policy are as follows:

Asset - Anything that has value to the organization.

Impact - An adverse change to the level of the organization's business objectives achieved.

Information security risk - The potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. It is measured in terms of a combination of the likelihood of an event and its consequence.

Residual risk – The risk remaining after risk treatment.

Risk owner – Person or entity with accountability and authority to manage a risk.

Risk assessment – The overall process of risk analysis and risk evaluation.

Risk avoidance – A decision not to become involved in, or action to withdraw from, a risk situation.

Risk communication - The exchange or sharing of information about risk between the decision-maker and other stakeholders.

Risk estimation – A process to assign values to the probability and consequences of a risk.

Risk identification – A process to find, list and characterize elements of risk.

Risk management – The coordinated activities to direct and control an organization with regards to risk.

Risk mitigation – Refer to “risk reduction”.

Risk reduction - Actions taken to lessen the probability, negative consequences or both, associated with a risk. Also referenced as “risk mitigation”.

Risk retention - Acceptance of the burden of loss or benefit of gain from a particular risk.

Risk transfer - Sharing with another party the burden of loss or benefit of gain, for a risk.

Risk treatment – The process for the selection and implementation of measures to mitigate risk.

5. Compliance Table

Policy/Procedure Name	ISO 27001:2022 Control	UAE IA Control	Requirements
Risk Management Procedure	A 6.1.2 & A 6.1.3		NIST SP800-144 Guidelines.

6. Review

The procedure needs to be reviewed by EFR once in a year, else whenever there are any changes implemented in the existing procedure.

7. ISMS Risk Statement

Information security risk management is an integral element of the overall ISMS framework at EFR. EFR is committed to safeguarding its assets by implementing processes & controls, documented in information security policies and procedures. This ensures security of the organization’s assets while minimizing risks. This is accomplished by:

- Promoting information security as a core value.
- Conducting timely risk assessments to gauge risks accurately and holistically.
- Focusing on the continuous improvement of operations.
- Complying with regulations and industry standards.

- Preventing and investigating the occurrence of security breaches.

The ISMS provides a formal, organized process whereby people plan, perform, assess, and improve processes to minimize risk and optimize information security. The ISMS applies to all personnel within the scope of the ISMS i.e., employees, contractors, and vendors as applicable.

8. Frequency of Risk Assessments

Risk assessments should be performed on half-yearly basis or upon any of the following events (may not be exhaustive):

- Changes to the risk management procedure.
- Changes to the ISMS scope.
- Major changes are contemplated to existing systems / assets.
- Major, sudden, or unplanned changes in senior management.
- Significant changes to the facilities or in cases where there is a relocation of facilities.
- New assets that have been included in the risk management scope.
- Necessary modification of asset values, e.g., due to changed business requirements.
- New threats that could be active both outside and inside the organization and that have not been assessed (changes to the threat landscape).
- Possibility that new or increased vulnerabilities could allow threats to exploit these new or changed vulnerabilities.
- Identified vulnerabilities to determine those becoming exposed to new or re-emerging threats.
- Increased impact or consequences of assessed threats, vulnerabilities and risks in aggregation resulting in an unacceptable level of risk.
- A security incident has occurred, or audit findings identify the need.
- As the risk assessment is a point in time review, it is imperative that risk assessments are frequently examined to ensure that changes in the business and operational environments are taken into consideration.

9. Responsibility and Authority

9.1 Management

The Steering Committee for ISO 27001 has the responsibility and authority to implement and enforce this procedure. In case, the organization puts a global risk management system across all departments/ functions, then it is the responsibility of the Steering Committee to ensure that the ISMS risk management approach is aligned with the risk management system of the organization.

Additionally, the Steering Committee has the responsibility to:

- Review and approve the risk assessment procedure and risk acceptance criteria, on a half yearly basis.

- Monitor the effectiveness of the risk management process.
- Ensure qualified and competent management is appointed to implement risk management processes.
- Review reports on the management of risks.
- The Steering Committee is responsible for ensuring that risk assessment is performed in a timely manner for the scoped areas to minimize risk. The Steering Committee members are responsible for ensuring that respective personnel reporting to him/her are compliant with applicable policies and procedures, standards, guidelines as well as regulations and legislation applicable to the ISMS.
- The Steering Committee is responsible for the development of risk treatment plans and the implementation of risk reduction strategies. Risk management processes should be integrated with other planning processes and management activities.

9.2 Responsibility Matrix

The following responsibility matrix clearly outlines how risk management responsibilities are laid out within the organization.

Sr. No.	Actions	Head of Operations	Technical Committee for ISO27001	Department SPOC or Managers	Staff
1	Asset Identification & Classification	I	R	C	I
2	Identification of threats and vulnerabilities	I	R	C	I/C
3	Assessment of threats and vulnerabilities	I	R	C	I
4	Identification and Evaluation for Risk Treatment Plan	I	R	C	I
5	*Risk Acceptance	I	R	C	I

* **Refer:** Annexure B for stakeholder group information.

Responsible - Performs the assessment. The person(s) assigned the job by the "A." Includes tactical responsibility for doing the work and completing the tasks.

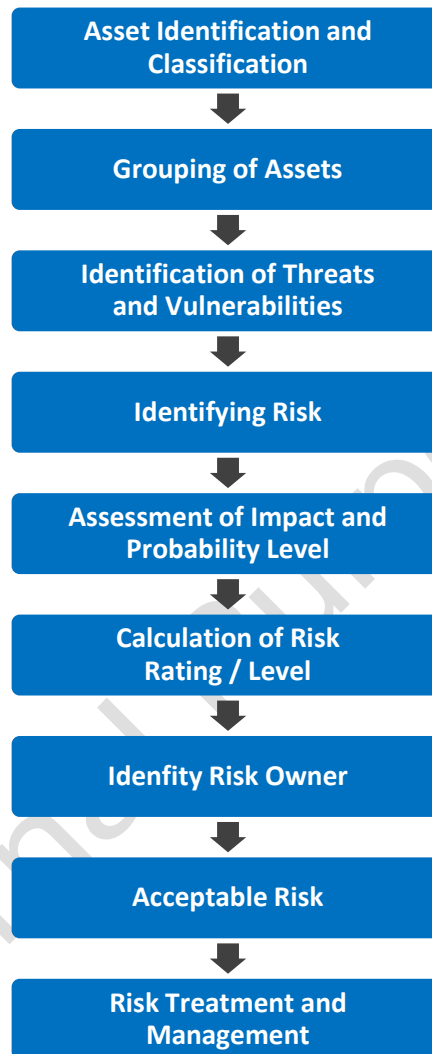
Contributing - Communicates the work (two-way). The person(s) who provide special support or should be consulted in making decisions or doing work.

Informed – Explains the work (one-way). The person(s) needing to be informed at key decision points during the work.

*Risk owners are responsible for the risk arising from/ through the assets; also responsible for risk treatment/acceptance criteria.

10. Risk Assessment Methodology

Risk Assessment at EFR will be done based on following steps



10.1 Asset Identification and Classification

The IT Team will identify all the Information assets of their respective department as part of the asset's identification exercise. All the assets that are identified by their respective stakeholders need to be classified according to their criticality based on confidentiality, integrity, and availability.

Assets shall be classified based on following criteria:

Asset Types	Definitions
Software	Software which is used to support / facilitate EFR's IT/ Business operations.

Asset Types	Definitions
Hardware	Physical devices/ enablers which are required / used to support EFR's operations.
Electronic Information	Information in any form (other than Physical hard copy), which is used / required/ generated during the course of operations and is used to manage business processes.
Facility & Service	Facilities/ Services/ Infrastructure which are necessary to ensure smooth operation.
People	People required to support & run operations.
Paper	Information in physical hard copy form, which is used/ required / generated during operations and is used to manage business processes.

The asset valuation scale is specified in terms of the level of damage or cost to the organization if an information security incident were to occur to an asset. The criterion considers:

- The level of classification of the impacted information asset.
- Breaches of information security (e.g., loss of confidentiality, integrity and availability).
- Impaired operations / system outages (internal or third parties).
- The loss of business and financial value.
- Disruption of plans and deadlines.
- Damage of reputation.
- Breaches of legal, regulatory or contractual requirements.

The following template shall be used for asset identification and risk assessment/ risk treatment (Refer **Annexure A**, the fields are detailed in the template).

The information asset owner will define the asset value, which will be adjudged by Technical Committee for ISO 27001 and approved by the Steering Committee for ISO 27001 if necessary. The assets will be valued differently based on Confidentiality, Integrity, and Availability. The asset owner will consider the following table while valuating assets.

Effect on Business	Impact	Rating
• What is the impact if information contained in the asset gets leaked? • What is the impact if information contained in the asset gets altered or deleted without authorization? • What is the impact if the Asset is not available?	Very Low	1
	Low	2
	Moderate	3
	High	4
	Very High	5

Asset value shall be calculated sum of C, I, A (Asset value=C+I+A), asset value greater than 4 shall be considered for risk assessment. Wherever possible the assets shall be combined and taken for risk

assessment, where deemed fit an assets value may also be escalated to achieve a minimum baseline in the group of assets being analyzed.

10.2 Grouping of Assets

The critical assets shall be grouped as per the following guidelines:

- Pick assets from the same business process
- Filter them based on the asset type
- They are then filtered based on same criticality ratings
- Shall also be grouped based on risk associated with assets

The grouping is primarily done as the group of assets would face similar types of threats and contain similar vulnerabilities faced by a particular asset would also be applicable to that group of assets. The highest asset value within a group shall be considered for calculation of the "Risk Rating" value.

10.3 Identification of Threats and Vulnerabilities

Information assets could be vulnerable and subject to many kinds of threats. Vulnerabilities are weaknesses associated with an organization's assets. These weaknesses may be exploited by a threat causing unwanted incidents that may result in loss, damage or harm to these assets. Vulnerability does not cause harm; it is merely a condition or a set of conditions that may allow a threat to affect an asset.

A threat has the potential to cause an unwanted incident, which may result in harm to a system or organization and its assets. This harm can occur from a direct or indirect attack on an organization's information e.g., its unauthorized destruction, disclosure, modification or loss. Threats can originate from accidental or deliberate sources or events. A threat would need to exploit the vulnerability of the systems, applications or services used by the organization to successfully cause harm to the asset.

All threats to the organization internal and external context shall be considered and the sources shall be taken from ISMS scope document, threat & vulnerability database from ARART template (**Refer:** Annexure A) and current market scenario.

10.4 Assessment of Threats

Threats are events that could cause harm to confidentiality, integrity or availability of the assets. Threats that could exploit system vulnerabilities shall be identified and analyzed for impact on EFR's information resources. Threats shall be classified into Very Low, Low, Moderate, High, or Very High based on the impact of threat, and following factors:

Threat Agents:

- Motivation of the Threat agent
- Perceived and required capabilities of the threat agent
- Resources available to the threat agent
- Perception of attractiveness to the threat agent

Threat Events:

- Probability of occurrence
- Geographical factors
- Environmental factors

Impact of threat level shall be classified based on the following table:

Impact	Level	Value
Extreme	Very High	5
Serious	High	4
Moderate	Moderate	3
Low	Low	2
Very Low	Very Low	1

Multiple threats are applicable to each asset group. Each threat has been individually mapped with the asset's groups and the average of the impact of multiple threats has been considered, i.e., "Average of Initial Impact Threat" for that group. The average value obtained will be further converted to the corresponding impact level as per the above table.

10.5 Assessment of Vulnerability

Vulnerabilities can be characterized as weaknesses in a system, or control gaps that, if exploited, could result in unauthorized disclosure, misuse, alteration or destruction of assets. Vulnerabilities associated with each threat shall be identified to produce a threat /vulnerability pair. The Threat/ Vulnerability analysis shall be performed on all information assets that are identified and classified and updated in the risk assessment register.

The probability of revised the vulnerability shall be classified based on the following table:

Probability	Level	Value
Almost Certain	Very High	5
Certain	High	4
Likely	Moderate	3
Possible	Low	2
Unlikely	Very Low	1

Multiple vulnerabilities are applicable to each threat, which have been mapped in "Threat Vulnerability Database". The maximum probability value for each group of vulnerability has been calculated in the "Vulnerability Database".

Further, while mapping the vulnerability with their corresponding threats (which were mapped to the asset groups), the average of maximum probability value of each vulnerability group has been obtained – i.e., "Average of Initial Probability". The average value obtained will be converted to the corresponding probability level as per the above table.

10.6 Calculation of Risk Rating

The risk rating of an asset shall be calculated based on the below procedure:

Risk Score = Probability * Impact

Asset Value (C+I+A)		
Confidentiality	Integrity	Availability
1	1	1
2	2	2
3	3	3
4	4	4
5	5	5

Threat Level	Vulnerability Level	Value
Very Low	Very Low	1
Low	Low	2
Moderate	Moderate	3
High	High	4
Very High	Very High	5

Risk Rating and Acceptance Table

	Vulnerability Level	Risk Rating	Acceptable ("Yes" or "No")	Value
Very Low	Very Low	0 to 5	Yes	1
Low	Low	5 to 10	Yes	2
Moderate	Medium	11 to 19	No	3
High	High	20 to 24	No	4
Very High	Very High	25 or higher	No	5

		RISK IMPACT				
		Insignificant 1	Minor 2	Significant 3	Major 4	Severe 5
RISK LIKELIHOOD	Almost Certain 5	Low 5	Low 10	Moderate 15	High 20	Very High 25
	Likely 4	Very Low 4	Low 8	Moderate 12	Moderate 16	High 20
	Moderate 3	Very Low 3	Low 6	Low 9	Moderate 12	Moderate 15
	Unlikely 2	Very Low 2	Very Low 4	Low 6	Low 8	Low 10
	Rare 1	Very Low 1	Very Low 2	Very Low 3	Very Low 4	Low 5

Based on the assessment of the grade of likelihood and impact, a score is calculated for each risk by multiplying the two numbers. This resulting score is then used to decide the classification of the risk based on the matrix shown.

Each risk will be allocated a classification based on its score as follows:

- Very High: 25 or more
- High: 20-24 inclusive
- Medium: 11 to 19 inclusive
- Low: 5 to 10 inclusive
- Very Low: 0 to 4 inclusive

10.7 Identify Risks

Based on the combination of threats and vulnerabilities, possible risks shall be identified against the assets. The possible risks may also be arrived at based on data captured as part of the ISO 27001 gap analysis, physical & environmental controls review, vulnerability assessments, business application review, technical application review, network security architecture reviews, internal audits etc.

10.8 Identify Risk Owner

Risk owners shall be assigned for each risk identified during the assessment. He/she will have accountability and authority to manage/mitigate the associated risk.

10.9 Acceptable Risk

Based on business drivers and the perception of risk in the industry, management shall determine the risks that are acceptable to the organization. Very low and low risks shall be treated as an acceptable risk and further action is not required in such cases.

10.10 Risk Treatment and Management

Identification and Evaluation Risk Treatment Plan

A risk treatment plan is prepared for moderate, high and very high levels of risks. The risk treatment shall be prioritized based on the resources needed - business impact/ Investment required/ Time required to implement the controls/ Complexity or difficulty associated with implementation – weighing these factors against the associated risks and benefits derived. Also, the existing controls are reviewed before necessary additional controls to mitigate the risk further are considered. These aspects are considered by the Steering Committee for ISO 27001 before arriving at a final decision, wherever necessary.

There are four possible ways of treating the risks, as detailed below:

- **Applying appropriate controls to reduce the risk**

To reduce the assessed risks appropriate and justified security controls should be identified and selected. The aim of control selection is to reduce risk to a level which is acceptable to EFR. This selection should be supported by the results of risk assessment. Already implemented controls should be re-examined in terms of cost comparisons, including maintenance, with a view to removing or improving them if they are not effective enough.

The **existing controls** and **additional controls** shall be mapped with respective ISO 27001 preventive/detective controls. After identifying controls, the impact and probability of the **threat and vulnerability level shall be revised**.

- **Avoiding the risks**

Risk avoidance describes any action where assets are moved away from risky areas. When evaluating the option of risk avoidance, it needs to be balanced against business and monetary needs. For e.g., it might be inevitable for an organization to use the Internet, despite all their concerns about hackers.

- **Transferring the associated risks to other parties**

Risk transfer might be the best option if it seems impossible to avoid the risk, and it is difficult or too expensive, to achieve appropriate reduction of risk. For e.g., risk transfer can be achieved by insuring or using third parties and outsourcing to partners to handle critical business assets.

- **Knowingly and objectively accepting risks, providing they clearly satisfy the IT security policy**

Risk acceptance criteria can be defined as the amount of risk, on a broad level, an entity is willing to accept in pursuit of its objectives. EFR has determined that it is willing to tolerate a certain level of risk exposure. The benefits to defining risk acceptance criteria for the organization are:

- Make better informed and risk-based decisions.
- Focus on the risks that exceed the defined acceptable level for risk.
- Develop a culture with a high awareness of risk.

For accepting the levels of risk detailed below, approvals from the person/body is required -

Risk Level	Acceptance Required From
Very High	- Board - Steering Committee for ISO 27001
High & Moderate	Steering Committee for ISO 27001
Low & Very Low	No approvals required

Evaluation of Residual Risk

The residual risk is the risk faced by the organization after implementing the controls. The residual risk shall be arrived based on the below formula.

Residual Risk= Highest asset value + Revised impact level + Revised probability level.

The residual risk can be categorized into very high, high, moderate, low and very low. EFR has decided that all residual very low or low risks which does not warrant further controls. However, if the residual risk is moderate, high or very high, measures shall be considered to further reduce risk levels by applying controls. In case the organization is unable to reduce risk in these cases, appropriate approvals and acceptance shall be obtained. This decision is based on the assets and risks involved and the impact on the business.

The residual risk shall be treated into four possible actions: Reduce risk, avoid risk, Transfer risk & Accept risk as detailed above.

Management Review

The periodic risk assessment review by the Steering Committee is an integral part of the cycle of ISMS for continual improvement. Any change taking place in the business model, organization structure, change in infrastructure, essentially calls for a management review of the risk assessment. Asset/ Risk assessment/ and Risk Treatment register will be used to centrally register, manage and track information security risks across EFR.

--End of Document--