Technical Guide

FAIR – ISO/IEC 27005 Cookbook

THE Open GROUP

Making standards work®

Technical Guide

FAIR – ISO/IEC 27005 Cookbook

ISBN: 1-931624-87-9

Document Number: C103

Published by The Open Group, October 2010.

Comments relating to the material contained in this document may be submitted to:

The Open Group
Thames Tower
37-45 Station Road
Reading
Berkshire, RG1 1LX
United Kingdom

or by electronic mail to:

ogspecs@opengroup.org

Contents

Preface

The Open Group

The Open Group is a vendor-neutral and technology-neutral consortium, whose vision of Boundaryless Information Flow™ will enable access to integrated information within and between enterprises based on open standards and global interoperability. The Open Group works with customers, suppliers, consortia, and other standards bodies. Its role is to capture, understand, and address current and emerging requirements, establish policies, and share best practices; to facilitate interoperability, develop consensus, and evolve and integrate specifications and Open Source technologies; to offer a comprehensive set of services to enhance the operational efficiency of consortia; and to operate the industry's premier certification service, including UNIX® certification.

Further information on The Open Group is available at www.opengroup.org.

The Open Group has over 15 years' experience in developing and operating certification programs and has extensive experience developing and facilitating industry adoption of test suites used to validate conformance to an open standard or specification.

More information is available at www.opengroup.org/certification.

The Open Group publishes a wide range of technical documentation, the main part of which is focused on development of Technical and Product Standards and Guides, but which also includes white papers, technical studies, branding and testing documentation, and business titles. Full details and a catalog are available at www.opengroup.org/bookstore.

As with all *live* documents, Technical Standards and Specifications require revision to align with new developments and associated international standards. To distinguish between revised specifications which are fully backwards-compatible and those which are not:

- A new *Version* indicates there is no change to the definitive information contained in the previous publication of that title, but additions/extensions are included. As such, it *replaces* the previous publication.

- A new *Issue* indicates there is substantive change to the definitive information contained in the previous publication of that title, and there may also be additions/extensions. As such, both previous and new documents are maintained as current publications.

Readers should note that updates – in the form of Corrigenda – may apply to any publication. This information is published at www.opengroup.org/corrigenda.

This Document

This document is the FAIR – ISO/IEC 27005 Cookbook. It has been developed and approved by The Open Group. This Guide is the third in a set of three Open Group publications addressing Risk Management:

- **The Open Group Technical Standard: Risk Taxonomy** provides a rigorous set of definitions and a taxonomy for information security risk, as well as information regarding how to use the taxonomy. The intended audience for this document includes anyone who has the need to understand and/or analyze a risk condition. This includes, but is not limited to:

  — Information security and risk management professionals

  — Auditors and regulators

  — Technology professionals

  — Management

- **The Open Group Technical Guide: Requirements for Risk Assessment Methodologies** identifies and describes the key characteristics that make up any effective risk assessment methodology, thus providing a common set of criteria for evaluating any given risk assessment methodology against a clearly defined common set of essential requirements. In this way, it explains what features to look for when evaluating the capabilities of any given methodology, and the value those features represent.

- **The Open Group Technical Standard: FAIR – ISO/IEC 27005 Cookbook** (this document) describes in detail how to apply the FAIR (Factor Analysis for Information Risk) methodology to any selected risk management framework. It uses ISO/IEC 27005 as the example risk assessment framework. FAIR is complementary to all other risk assessment models/frameworks, including COSO, ITIL, ISO/IEC 27002, COBIT, OCTAVE, etc. It provides an engine that can be used in other risk models to improve the quality of the risk assessment results. The Cookbook enables risk technology practitioners to follow by example how to apply FAIR to other risk assessment models/frameworks of their choice.

Intended Audience

The primary target audience for this Cookbook is risk management analysts and practitioners, to help them to use ISO/IEC 27005 to achieve higher quality risk assessment results, especially given the lack of formal specificity in probabilism provided by ISO/IEC 27005, including in its difficult appendices on creation of a probabilistic model.

Trademarks

Boundaryless Information Flow™ and TOGAF™ are trademarks and Making Standards Work®, The Open Group®, UNIX®, and the "X" device are registered trademarks of The Open Group in the United States and other countries.

COBIT® is a registered trademark of the Information Systems Audit and Control Association and the IT Governance Institute.

ITIL® is a registered trademark of the Office of Government Commerce in the United Kingdom and other countries.

OCTAVE® is a registered trademark of Carnegie Mellon University.

The Open Group acknowledges that there may be other brand, company, and product names used in this document that may be covered by trademark protection and advises the reader to verify them independently.

Acknowledgements

The Open Group gratefully acknowledges the contribution of the following people in the development of this document:

- Lead Authors:

  — Christopher Carlson, The Boeing Company

  — Alex Hutton, Verizon

- Contributing Author:

  — Anastasia Gilliam, Independent Consultant

- Reviewers:

  — Members of the Security Forum, The Open Group

Referenced Documents

The following documents are referenced in this Guide:

- ISO/IEC 27005:2008: Information Technology – Security Techniques – Information Security Risk Management.
- ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management System – Requirements (ISMS).
- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management (Controls).
- Technical Standard: Risk Taxonomy (C081, ISBN: 1-931624-77-1), January 2009, published by The Open Group.
- Technical Guide: Requirements for Risk Assessment Methodologies (G081, ISBN: 1-931624-78-X), January 2009, published by The Open Group.

1 Introduction

1.1 Purpose

The purpose of this document is to help the security practitioner responsible for their organization's risk estimation function to utilize The Open Group Risk Management Framework in an ISO/IEC 27005 structured process. This document discusses the different purposes of the two standards, how to reconcile the two with regard to terminology and process, and combine the best elements of both to produce a consistent, repeatable risk management process.

1.2 Scope

This document does not fully discuss the role of risk management in the context of the security executive's portfolio, the communication of risk, nor the use of metrics in risk estimation or risk management. Rather, it is solely focused on risk management and risk estimation, and how the practitioner can combine FAIR (Factor Analysis for Information Risk) and ISO/IEC 27005 into a robust business process. The examples and "cookbook" approach are designed to give the risk analyst a pragmatic and repeatable process applicable to most of their daily tasks.

1.3 Intended Audience

Although this document addresses ISO/IEC 27005, it is not written in a style and discipline that is consistent with an ISO publication. Instead, it is written in the style of its companion Open Group Risk Management publications:

- Risk Taxonomy Technical Standard
- Requirements for Risk Management Methodologies Technical Guide

because, like its companion publications, its primary target audience is people who actually "do" risk management rather than write ISO standards.

In this regard, some consideration has been given to the notion that anyone interested in presenting this Cookbook using the ISO style and discipline could re-write it so as to position it as an SC27 TR, and thereby perhaps make it more attuned to the expectations of the ISO standards community and its worldwide audience.

1.4 Operating Assumptions

It is assumed that:

- The reader is familiar with ISO/IEC 27001 and ISO/IEC 27002.

- The reader is thoroughly familiar with ISO/IEC 27005, and is experienced in using it.
- The reader knows the FAIR risk management approach, as defined in the referenced Open Group Risk Taxonomy Technical Standard, and is familiar with using it.

Clearly the reader with good understanding of risk management and its role in an information security program will be at a considerable advantage. In this respect, the referenced Open Group Requirements for Risk Assessment Methodologies Technical Guide is a recommended reference.

1.5 Using this Cookbook

One of the most significant issues with the current state of information risk management is lack of established nomenclature. Terms like “threat”, “impact”, and even “risk” can carry different perspectives and meanings. The first thing the reader may find best to do is review Table 2 in Section 2.3 to reconcile terms into a common taxonomy and ontology. Once the reader has digested that information, it may then be advisable to quickly review ISO/IEC 27005 §5 before returning to Section 2, though this step is not “required”. After reading and following the examples given, the reader is encouraged to attempt risk analysis for themselves using the example as a guideline and Appendix A to this document as a template.

In the context of security portfolio management, this document may be applicable to the following enterprise functions:

- Project management
- Resource prioritization
- Security architecture development
- Compliance solution development
- Control solution development

2 How to Manage Risk

2.1 ISMS Overview

The reader should already understand that the ISO Information Security Management System (ISMS) is intended to be an organization’s strategic plan for information security. This section provides a brief overview of the relevant ISO documents. The relationship of the concepts is shown in Figure 1.

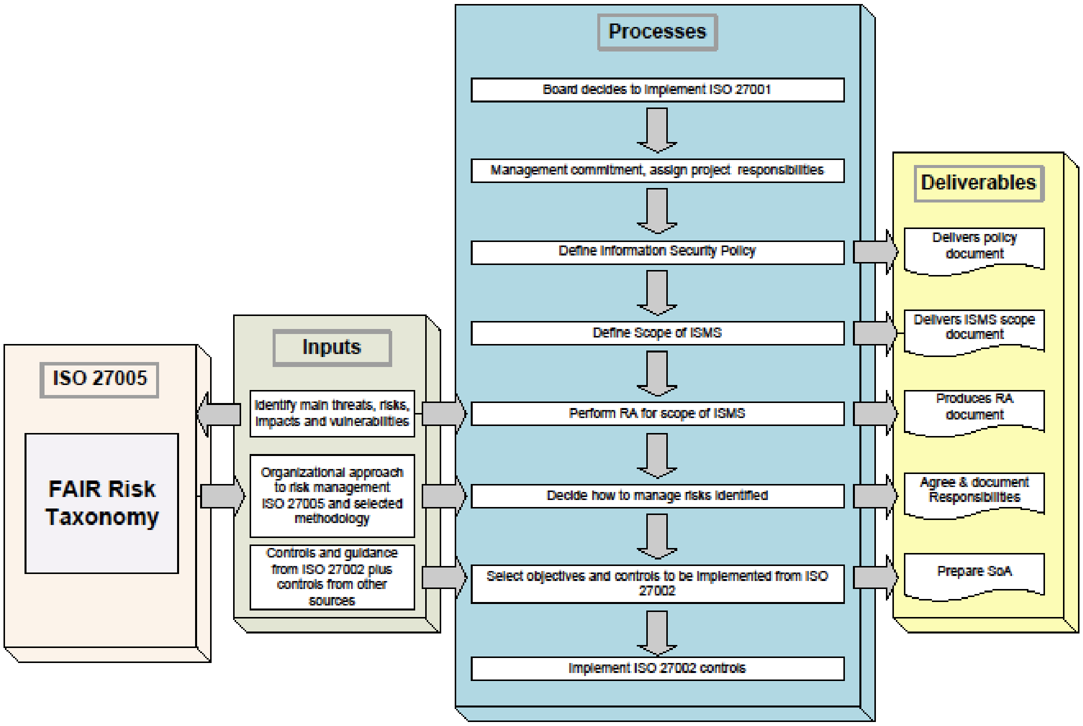

Processes
Board decides to implement ISO 27001
Management commitment, assign project responsibilities
Define Information Security Policy
Define Scope of ISMS
Perform RA for scope of ISMS
Decide how to manage risks identified
Select objectives and controls to be implemented from ISO 27002
Implement ISO 27002 controls
Deliverables
Delivers policy document
Delivers ISMS scope document
Produces RA document
Agree & document Responsibilities
Prepare SoA
ISO 27005
FAIR Risk Taxonomy
Inputs
Identify main threats, risks, impacts and vulnerabilities
Organizational approach to risk management ISO 27005 and selected methodology
Controls and guidance from ISO 27002 plus controls from other sources

Figure 1: Use of ISO/IEC 27005 and FAIR in ISO/IEC 27001 ISMS Development Processes

ISO provides several documents that offer guidance in developing the ISMS. Those relevant to management of risk are:

- ISO/IEC 27001:2005: Information Technology – Security Techniques – Information Security Management System – Requirements (ISMS):

  — Describes a model for establishing, implementing, operating, monitoring, reviewing, maintaining, and improving an ISMS

  — Used to assess conformance by interested internal and external parties

— Applies to all types of organizations (e.g., commercial enterprises, government agencies, non-profit organizations)

— Ensures selection of adequate and proportionate security controls that protect information assets and give confidence to interested parties

— Specifies requirements for the implementation of security controls customized to the needs of individual organizations or departments

- ISO/IEC 27002:2005: Information Technology – Security Techniques – Code of Practice for Information Security Management (Controls):

  — Provides 12 domains of information security

  — Defines security controls that may be selected within each domain

  — Provides implementation guidance in each area

- ISO/IEC 27005:2008: Information Technology – Security Techniques – Information Security Risk Management:

  — Provides a general approach to risk management

  — Is the primary focus of this document

Since the ISMS is a strategic plan for information security, its development is influenced by the needs and objectives, security requirements, processes, and the size and structure of the organization. Each company's ISMS (and the organization's security environment) is expected to change over time; consequently, ISO's implementation of ISMS uses the "Plan-Do-Check-Act" (PDCA) model. See ISO/IEC 27001 §0.2 for the PDCA model as applied to the ISMS.

Stages of the PDCA model are as follows:

- **Plan** (establish the ISMS): Establish ISMS policy, objectives, processes, and procedures relevant to managing risk and improving information security to deliver results in accordance with an organization's overall policies and objectives.

- **Do** (implement and operate the ISMS): Implement and operate the ISMS policy, controls, processes, and procedures.

- **Check** (monitor and review the ISMS): Assess and, where applicable, measure process performance against ISMS policy, objectives, and practical experience and report the results to management for review.

- **Act** (maintain and improve the ISMS): Take corrective and preventive actions, based on the results of the internal ISMS audit and management review or other relevant information, to achieve continual improvement of the ISMS.

An ISMS implementation should be scaled in accordance with the organization's needs – a simple situation requires a simple ISMS solution. For an organization to claim conformance to ISO/IEC 27001, none of the requirements specified in Clauses 4, 5, 6, 7, and 8 may be excluded. Any exclusion of controls found to be necessary to satisfy the risk acceptance criteria needs to be justified and evidence needs to be provided that the associated risks have been accepted by the accountable persons. Where any controls are excluded, claims of conformance to ISO/IEC

27001 are not acceptable unless such exclusions do not affect the organization's ability, and/or responsibility, to provide information security that meets the security requirements determined by risk assessment and applicable legal or regulatory requirements.

2.2 How FAIR Plugs into the ISMS

ISO/IEC 27001 describes a general process for the ISMS, and in that context ISO/IEC 27005 defines the approach to managing risk. FAIR provides a methodology for analyzing risk. This section describes how the FAIR methodology can be used to analyze risk in the context of ISO/IEC 27005 and the ISMS. Step-by-step details based on these concepts are presented in ISO/IEC 27005 §5.

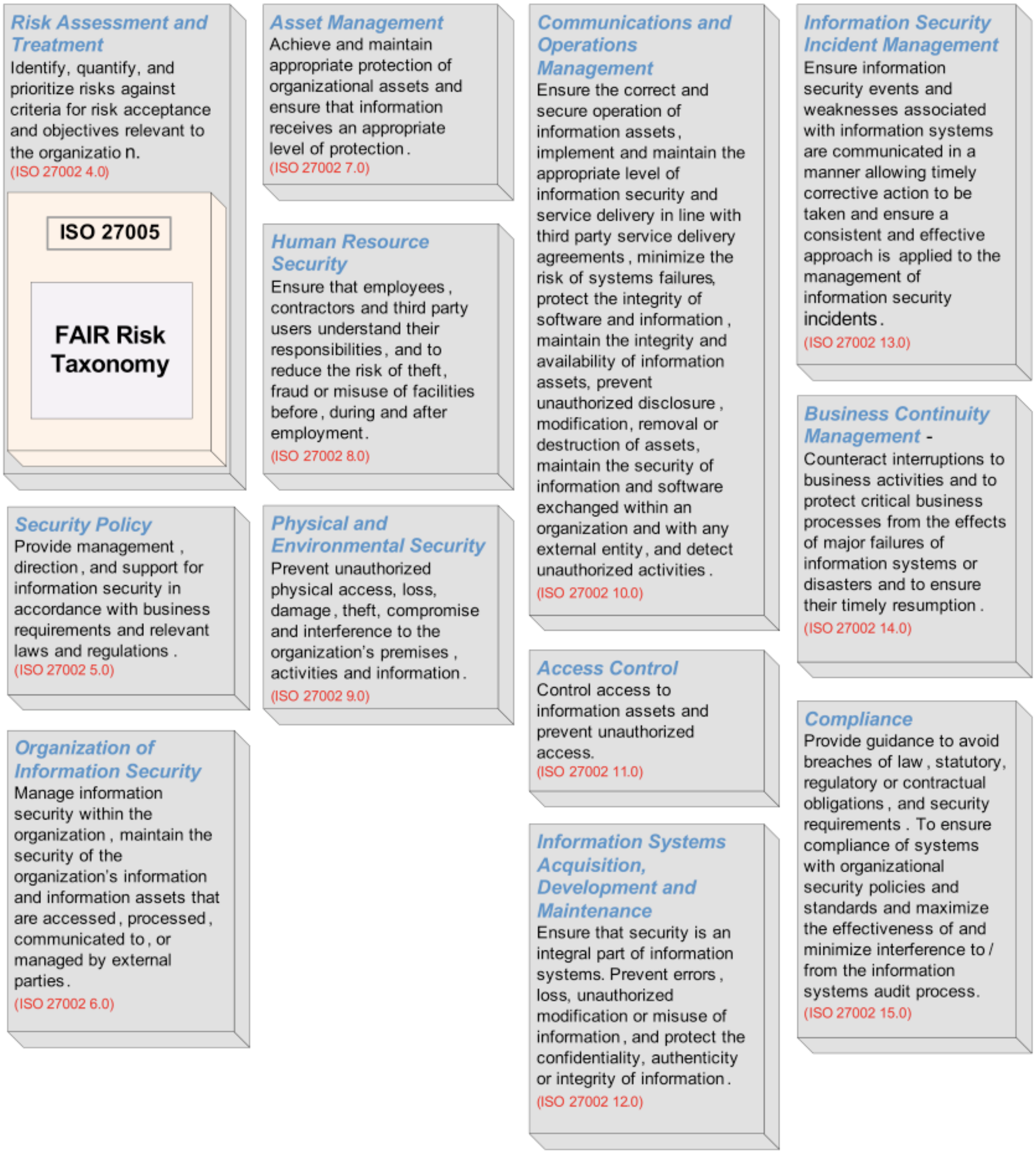
ISO/IEC 27001 §4.2.1 provides the foundation for the risk management portion of the ISMS:

- Define the risk assessment approach of the organization
- Identify the risks
- Analyze and evaluate the risks
- Identify and evaluate options for the treatment of risks
- Select control objectives and controls for the treatment of risks
- Obtain management approval of the proposed residual risks

This generally outlines the process for managing risk at a very high level.

ISO/IEC 27002 provides the taxonomy of information security controls. Figure 2 illustrates how the FAIR framework complements the ISO/IEC 27002 framework. ISO/IEC 27002 §4.0 discusses risk management and treatment as a domain in the ISMS.

ISO/IEC 27005 specifies in more detail the management of risk without providing specifics or identifying a methodology for determining risk level. FAIR provides a methodology to achieve the steps shown above, specifically "identify the risks" and "analyze and evaluate the risks".



Risk Assessment and Treatment
Identify, quantify, and prioritize risks against criteria for risk acceptance and objectives relevant to the organizatio n.
(ISO 27002 4.0)

ISO 27005

FAIR Risk Taxonomy

Security Policy
Provide management , direction , and support for information security in accordance with business requirements and relevant laws and regulations .
(ISO 27002 5.0)

Organization of Information Security
Manage information security within the organization , maintain the security of the organization's information and information assets that are accessed , processed , communicated to , or managed by external parties .
(ISO 27002 6.0)

Asset Management
Achieve and maintain appropriate protection of organizational assets and ensure that information receives an appropriate level of protection .
(ISO 27002 7.0)

Human Resource Security
Ensure that employees , contractors and third party users understand their responsibilities , and to reduce the risk of theft , fraud or misuse of facilities before , during and after employment .
(ISO 27002 8.0)

Physical and Environmental Security
Prevent unauthorized physical access, loss, damage , theft, compromise and interference to the organization's premises , activities and information .
(ISO 27002 9.0)

Communications and Operations Management
Ensure the correct and secure operation of information assets , implement and maintain the appropriate level of information security and service delivery in line with third party service delivery agreements , minimize the risk of systems failures, protect the integrity of software and information , maintain the integrity and availability of information assets, prevent unauthorized disclosure , modification, removal or destruction of assets, maintain the security of information and software exchanged within an organization and with any external entity , and detect unauthorized activities .
(ISO 27002 10.0)

Access Control
Control access to information assets and prevent unauthorized access.
(ISO 27002 11.0)

Information Systems Acquisition, Development and Maintenance
Ensure that security is an integral part of information systems. Prevent errors , loss, unauthorized modification or misuse of information , and protect the confidentiality, authenticity or integrity of information .
(ISO 27002 12.0)

Information Security Incident Management
Ensure information security events and weaknesses associated with information systems are communicated in a manner allowing timely corrective action to be taken and ensure a consistent and effective approach is applied to the management of information security incidents .
(ISO 27002 13.0)

Business Continuity Management -
Counteract interruptions to business activities and to protect critical business processes from the effects of major failures of information systems or disasters and to ensure their timely resumption .
(ISO 27002 14.0)

Compliance
Provide guidance to avoid breaches of law , statutory, regulatory or contractual obligations , and security requirements . To ensure compliance of systems with organizational security policies and standards and maximize the effectiveness of and minimize interference to / from the information systems audit process.
(ISO 27002 15.0)

Figure 2: FAIR Integrated into ISO/IEC 27002 ISMS Controls Framework

Table 1 shows how the FAIR risk analysis steps relate to the process outlined in ISO/IEC 27005.

Table 1: FAIR's Place within ISO/IEC 27005

7.0	Context Establishment	
7.1	General Considerations	
7.2	Basic Criteria	
7.3	Scope and Boundaries	
7.4	Organization of Information Security Risk Management	
8.0	Information Security Risk Assessment	
8.1	General Description of Information Security Risk Assessment	
8.2	Risk Analysis	**Risk Analysis using FAIR** Stage 1: Identify scenario components Identify the asset at risk Identify the threat community Stage 2: Evaluate Loss Event Frequency (LEF) Estimate probable Threat Event Frequency (TEF) Estimate Threat Capability (TCap) Estimate Control Strength (CS) Derive Vulnerability (Vuln) Derive Loss Event Frequency (LEF) Stage 3: Evaluate Probable Loss Magnitude (PLM) Estimate worst-case loss Estimate Probable Loss Magnitude (PLM) Stage 4: Derive and articulate risk
8.2.1	Risk Identification	
8.2.1.1	Introduction to risk identification	
8.2.1.2	Identification of assets	
8.2.1.3	Identification of threats	
8.2.1.4	Identification of existing controls	
8.2.1.5	Identification of vulnerabilities	
8.2.1.6	Identification of consequences	
8.2.2	Risk estimation	
8.2.2.1	Risk estimation methodologies	
8.2.2.2	Assessment of consequences	
8.2.2.3	Assessment of incident likelihood	
8.2.2.4	Level of risk estimation	
8.3	Risk Evaluation	
9.0	Information Security Risk Treatment	
9.1	General Description of Risk Treatment	
9.2	Risk Reduction	
9.3	Risk Retention	
9.4	Risk Avoidance	
9.5	Risk Transfer	
10.0	Information Security Risk Acceptance	
11.0	Information Security Risk Communication	
12.0	Information Security Risk Monitoring and Review	
12.1	Monitoring and Review of Risk Factors	
12.2	Risk Management Monitoring, Reviewing, and Improving	

While ISO/IEC 27001 outlines the process for managing risk at a very high level, by defining the ISMS, ISO/IEC 27005 specifies in more detail the management of risk, although without providing specifics or identifying a methodology for determining risk level. You can see how FAIR fills the gap in ISO/IEC 27005 §8.2 and §8.3 by providing the detailed methodology for risk assessment and risk evaluation, and is a strong compliment to the ISO/IEC 27005 process in support of the ISMS.

ISO/IEC 27005 does provide guidelines for development of risk assessment context, risk communication, and treatment, but it does not provide a methodology for determining the nature and impact of the actual risk (risk assessment methodology). FAIR does provide such a methodology for determining the nature and impact of the actual risk. The combination of ISO/IEC 27005 and FAIR can therefore serve as the framework and methodology for the risk evaluation and analysis processes domain. Figure 3 illustrates the integration of FAIR in the ISO/IEC 27005 framework.

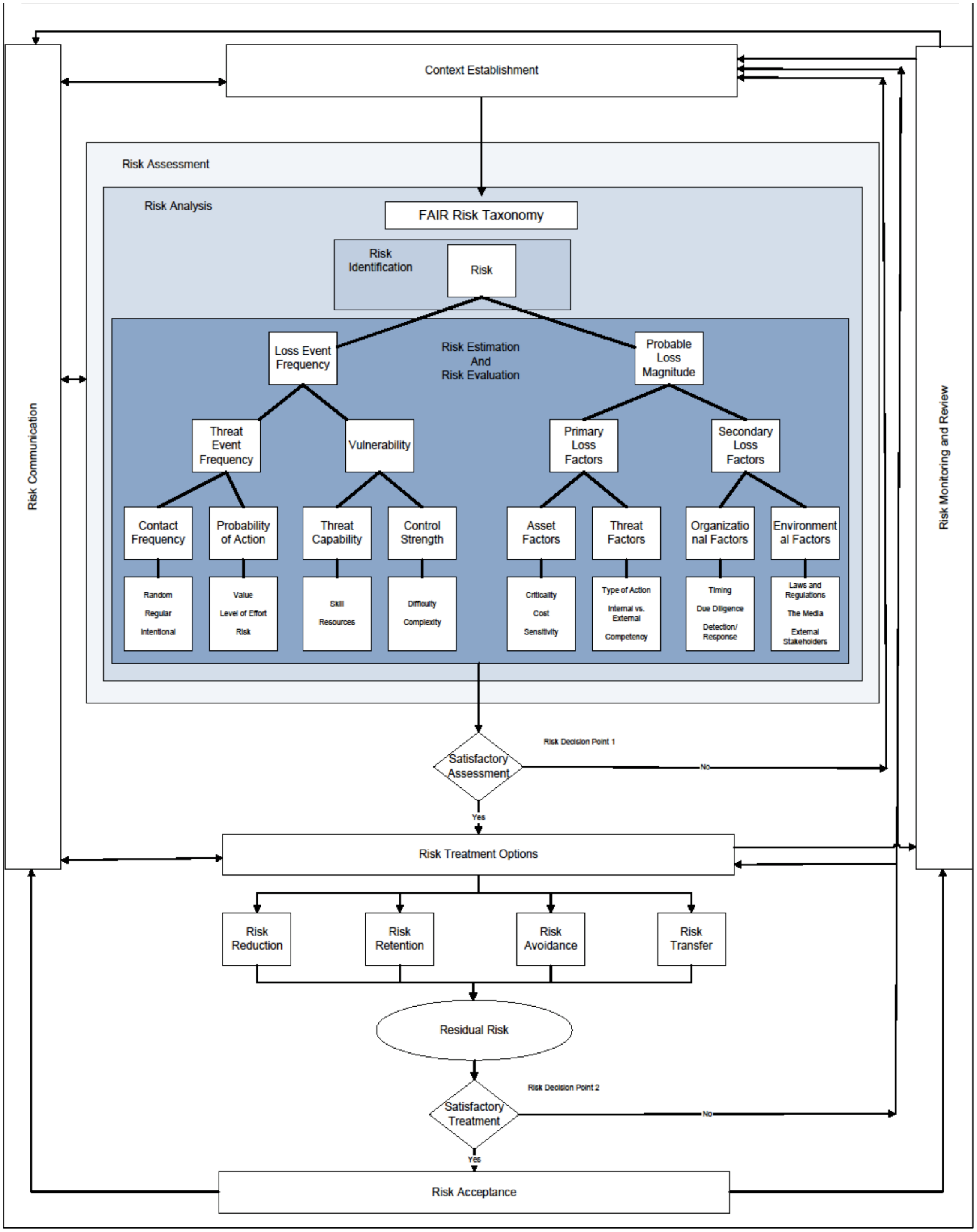


Figure 3: ISO/IEC 27005 – FAIR Integration Model

2.3 Major Differences in Approach

There are numerous differences between ISO/IEC 27005 and FAIR. However, the standards complement each other in many ways. ISO/IEC 27005 provides a framework for a risk management program. It includes concepts such as risk management program development, risk management communication, monitoring, and treatment of risks. FAIR provides an actual methodology for evaluating the probabilities and impacts of actual risks. In other words, FAIR provides the actual methods to meet the needs of ISO/IEC 27005 §8.2 (Risk Analysis) and §8.3 (Risk Evaluation). This can be seen graphically in Figure 2 above.

Other differences exist in such items as specific definitions. The following definition differences are dominant:

Table 2: Differences in ISO/IEC 27005 and FAIR Definitions

Term	FAIR Definition	ISO Definition	Specific ISO Reference	Differences
Asset	Any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.	Anything that has value to the organization.	ISO/IEC 27001 ISO/IEC 27002	ISO provides a simpler, but somewhat vague definition of asset. The FAIR definition looks at assets from the perspective of information security and the principles of confidentiality, integrity, and availability.
Risk	The probable frequency and probable magnitude of future loss.	Combination of the probability of an event and its consequence.	ISO/IEC 27002	These two definitions are nearly identical. The concepts of magnitude and consequence are synonymous. The ISO use of probability can be interpreted as likelihood, while FAIR deliberately uses frequency.
Threat	Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.	A potential cause of an unwanted incident, which may result in harm to a system or organization.	ISO/IEC 27002	These two definitions are nearly identical.

Term	FAIR Definition	ISO Definition	Specific ISO Reference	Differences
Vulnerability	The probability that an asset will be unable to resist actions of a threat agent.	A weakness of an asset or group of assets that can be exploited by one or more threats.	ISO/IEC 27002	ISO focuses on the existence of a weakness whereas FAIR focuses on the asset's ability to resist the actions of a threat agent.

2.4 Recommended Approach

The first step in any risk analysis is to identify the question(s) to be answered. An organization that wants to identify and prioritize security technology investments needs to understand which controls are most important to reduce risk; that is, which controls have both the most influence on risk and are in greater need of improvement. The ISMS defines the management system for establishing a context for risk, and for managing risk decisions. ISO/IEC 27002 provides a taxonomy of security controls, complete with guidelines for evaluating control effectiveness. ISO/IEC 27005 provides the framework for risk management and FAIR provides the methodology for evaluating and quantifying risk. In the following sections we will see how the integration of ISO/IEC 27005 and FAIR provides a method for calculating risk so that these questions can be answered for business owners.

2.5 Points to Consider

2.5.1 Concerns Regarding Complexity of the Model

The incorporation of FAIR and ISO/IEC 27005 makes for a more complex model than either standard alone. ISO’s high-level approach to risk management (determining the context, developing treatment and communications plans), while essential to risk management, adds to the tasks of FAIR.

The FAIR framework goes into greater detail than most risk models. This level of detail provides some advantages:

- Flexibility to go deep when necessary
- Better understanding of factors contributing to risk
- Ability to better troubleshoot analysis performed at higher layers of abstraction

However, if usage of FAIR required analyses at the deepest layers of granularity it would be impractical for risk analysis. Fortunately, FAIR risk assessment can be performed using data/estimates at higher levels of abstraction within the model (for example, measuring Threat Event Frequency (TEF) rather than attempt to measure contact frequency and probability of action). Flexibility within the framework enables the user to choose the appropriate level of analysis, based on the time, data, complexity, and significance of the scenario.

Another consideration relating to complexity is that risk by its very nature is inherently complicated. Over-simplified models lead to false conclusions and recommendations. FAIR’s detailed taxonomy may not be a perfect treatment of the problem, but FAIR is considered to be the most complete, best analyzed, and defined methodology/taxonomy available.

Communicating complex risk information to decision-makers presents a problem with any model. As with any complex problem, it is important to articulate results in ways that can be processed most easily and so are most useful to decision-makers. Having a rigorous framework and explaining how the results were arrived at improves credibility and acceptance of the results. Developing a communication plan as prescribed in ISO/IEC 27005 provides guidance to ensure the appropriate information is dispersed to all identified stakeholders.

2.5.2 Availability of Data to Support Statistical Analysis

In risk assessment, quality data is difficult to acquire. In the absence of such data, it is hard to achieve valid frequency estimates. This challenge partially originates from the absence of a detailed framework that:

- Defines which metrics are needed
- Provides a model for incorporating the data so that meaningful results can be obtained

2.5.3 The Iterative Nature of Risk Analyses

Due to the inherent complexity of risk, analyses tend to be iterative in nature. In other words, developing a treatment plan can introduce other risks that must be evaluated. With each iteration the results become more precise, but there comes a point of diminishing returns beyond which additional precision and evaluation is not warranted given the necessary time and expense of further analyses.

3 What Information is Necessary for Risk Analysis?

3.1 Introduction to the Landscape of Risk

In general, any risk management/analysis/estimation exercise is an attempt to reconcile the relationships between four dependent sources of information – threat, loss (impact), controls, and assets – into a descriptive point of reference called "risk". Each risk management standard or methodology treats these information "landscapes" in a somewhat subtly different manner from others. For the purposes of helping analysts augment ISO/IEC 27005 processes with a FAIR-based risk estimation, we will begin by comparing the approaches of each standard for each landscape, and discussing in general terms what sort of prior information may contribute to providing context for the factors needed in a FAIR estimation.

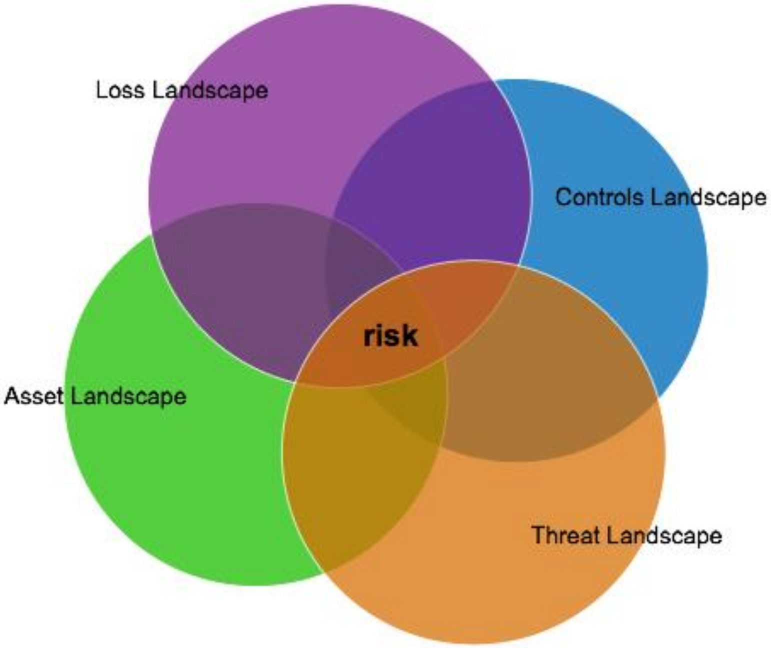


Figure 4: Risk Landscapes

3.2 Asset Landscape

The asset landscape represents information concerning that which is to be protected. To perform a FAIR analysis, the analyst needs to understand the nature of the asset in question and how it relates to each of the other landscapes.

As the asset intersects with the loss or impact landscape, the analyst should understand information including: the business process(es) the asset contributes to, the cost to replace the asset, the architecture of the asset (hardware, software, nature of services accessible, etc.), and the resources necessary to respond to an incident (geographic location in relation to the Incident Response Team, for example).

In considering the threat landscape, the analyst may find it useful to pre-suppose the applicable threat community. In doing so, information about the asset's value to the threat can be considered, as well as the relative frequency and nature of threat contact with the asset in question.

Finally, the analyst should seek to understand aspects of the asset that will contribute to the ability to resist the actions of a threat agent (for example, the architecture of some assets may be more or less prone to vulnerability than others). It may seem to be a semantic distinction, but information regarding the nature of the asset and the organization's ability to manage and maintain the asset contribute to our understanding of the controls landscape.

Other information is useful in generating a generalized "context" as per ISO/IEC 27005, such as the list given on page nine of that document (repeated here for convenience):

- The organization's strategic business objectives, strategies, and policies
- Business processes
- The organization's functions and structure
- Legal, regulatory, and contractual requirements applicable to the organization
- The organization's information security policy
- The organization's overall approach to risk management
- Information assets
- Locations of the organization and their geographical characteristics
- Constraints affecting the organization
- Expectation of stakeholders
- Socio-cultural environment
- Interfaces (i.e., information exchange with the environment)

3.2.1 ISO Definition and Goal

ISO/IEC 27005 defines asset as "anything that has value to the organization and which therefore requires protection". The asset identification described in ISO/IEC 27005 §8.2.1.2 suggests that asset identification should be performed at a suitable level for the risk assessment, and that the owner should be identified for each asset. The output of ISO/IEC 27005 §8.2.1.2 is a list of the assets to be risk managed and a list of business processes related to assets and their relevance.

3.2.2 Major Differences in Asset Landscape Treatment

The identification of assets for analysis and creation of an asset catalog that includes asset owners and the business processes assets support is useful for analysis using both standards.

3.3 Threat Landscape

The threat landscape consists of the information we need to understand concerning those which may act against our asset.

3.3.1 ISO Definition and Goal

A threat has the potential to harm assets such as information, processes and systems, and therefore, organizations. Threats may be of natural or human origin, and could be accidental or deliberate.

The output is a list of threats with the identification of threat type and source.

3.3.2 Major Differences in Threat Landscape Treatment

The most significant differences in threat landscape treatment between The Open Group probabilistic approach and the ISO/IEC 27005 process are:

- The structure of classification
- The consideration of threat actions
- The development of metrics for the threat landscape

3.3.3 Structure of Classification

ISO/IEC 27005 treats the concept of a threat as either a cause or effect which can be confusing, and lead to significantly more work than is needed to define the relevant aspects of the threat landscape. The Open Group approach breaks threats down by category (human/natural/malware) and then by characteristics (physical and trust relationships to the controls and assets).

An analyst can utilize The Open Group framework's more rational, descriptive structure in their analysis. This would mean identifying the most probable threat for consideration from one of the following categories:

Human			
Internal	**External**	**Malware**	**Force Majeure**
Privileged	Technical Professional	Any self-propagating	Various
Non-Privileged	Technical Amateur		
	Non-Technical Professional		
	Non-Technical Amateur		

3.3.4 Consideration of Threat Actions

The Open Group framework does not specifically address threat actions. An analyst can utilize the ISO/IEC 27005 list to describe the action that the threat source is most likely to take. The action consideration would then help the analyst to establish metric ranges for the threat landscape.

In our example, given our asset "A" we might ascribe threat action "SQL injection" to the threat community "External Technical Professional". Other external threat frameworks (for example, WASC for web-based attacks) can also be used to describe threat actions within the context of threat modeling for this landscape.

3.3.5 The Development of Metrics for the Threat Landscape

To create a probabilistic approach to risk estimation, The Open Group framework requires estimated ranges for two specific metrics:

1. The expected frequency of "threat events"
2. The ability of the threat to apply force against the asset and subsequent controls, or "threat capability"

In developing these threat metrics, the threat classification and probable threat actions should drive the analyst's quest for evidence and subsequent measurements.

In our example, an analyst might seek frequency numbers for SQL injection attempts against asset "A" or significantly similar assets, and then ascribe a range for threat capability based on the strength/complexity of that attack type when compared to other attacks that asset may face.

Once the metrics for the threat landscape are gathered, the next step in risk analysis would be to review the controls landscape, as the ability to resist controls is relative to threat capability (which FAIR defines as the level of force we might expect a threat agent to apply against an asset).

3.4 Controls Landscape

3.4.1 ISO Definition and Goal

ISO/IEC 27005 §8.2.1.4 discusses what is useful for the identification of existing or planned controls for consideration in risk analysis. The input for ISO/IEC 27005 §8.2.1.4 is control documentation and potential risk treatment plans, and the output is a list of all existing and planned controls, their implementation, and usage status.

3.4.2 Major Differences in Controls Landscape Treatment

The controls landscape in ISO/IEC 27005 is better defined as what is governed in ISO/IEC 27001. Controls in ISO/IEC 27005 are estimated in "effectiveness" based on their ability to reduce the likelihood and/or ease of vulnerability exploit, and/or the impact of an incident. We might say that in ISO/IEC 27005 controls are judged relative to the exploit (ignoring for a moment a control that reduces impact).

Controls in FAIR are defined as those things that will contribute to an ability to resist a threat community. Control strength is an estimation of the ability to resist the force applied by some percentage of the general threat agent population. We might say that in FAIR an ability to resist is judged relative to the threat population.

3.4.3 Development of Metrics for the Controls Landscape

The primary metric for use in FAIR analysis is control strength. Control strength should be measurement of the ability to resist the force applied by some percentage of the general threat agent population. Information in ISO/IEC 27005 §8.2.1.4 (implementation and usage information) suggests that analysts should gather "control effectiveness" ratings for various controls that are useful in establishing control strength estimates.

3.5 Loss (Impact) Landscape

3.5.1 ISO Definition and Goal

ISO/IEC 27005 defines impact as an adverse change to the level of business objectives achieved. ISO/IEC 27005 §8.2.1.6 discusses the identification of consequences that losses of confidentiality, integrity, and availability may have on the assets. A consequence can be loss of effectiveness, adverse operating conditions, loss of business, reputation, damage, etc.

3.5.2 Major Differences in Loss (Impact) Landscape Treatment

Both approaches share the common challenge of attempting to estimate the value of a loss event.

The loss (impact) landscape in ISO/IEC 27005 uses the technique of incident scenarios (also called security failures in ISO/IEC 27001). Impacts in ISO/IEC 27005 are identified by estimating the damage or consequences to the organization that could be caused by an incident scenario. So ISO produces a list of possible impacts presented as discrete values sometimes expressed as monetary values.

FAIR focuses on identifying the factors that drive loss magnitude when events occur. An asset's loss potential stems from the value it represents and/or the liability it introduces to an organization. So, FAIR presents loss as a mathematical model of a range of likely monetary values.

3.5.3 Structure of Classification

Forms of loss come from two sources. First, there are losses that are primarily (or directly) incurred due to the actions of the threat agent – a lack of productivity, destruction of assets, the cost of incident response. Second, there are losses that an organization encounters when another party acts because of the primary losses – losses that occur due to regulatory fines, class action lawsuits, losses in revenue due to customer churn, etc. Both FAIR and ISO/IEC 27005 classify loss forms in a similar manner, aiding the development of metrics for the loss or impact landscape.

3.5.4 Development of Metrics for the Loss (Impact) Landscape

Annex B of ISO/IEC 27005 guides readers to develop loss assessments based on “direct” and “indirect” operational impacts. Similarly, FAIR breaks down loss forms into primary and secondary loss categories. Table 3 compares these categories:

Table 3: Comparison of Loss Categories

FAIR – Primary Losses	**ISO/IEC 27005 Direct Operational Impacts**
Productivity: The reduction in an organization’s ability to generate its primary value proposition (e.g., income, goods, services, etc.).	The financial replacement value of lost (part of) asset.
Response: Expenses associated with managing a loss event (e.g., internal or external person-hours, logistical expenses, etc.).	The cost of acquisition, configuration, and installation of the new asset or back-up.
Replacement: The intrinsic value of an asset. Typically represented as the capital expense associated with replacing lost or damaged assets (e.g., rebuilding a facility, purchasing a replacement laptop, etc.).	The cost of suspended operations due to the incident until the service provided by the asset(s) is restored.
	Impact results in an information security breach.
FAIR – Secondary Losses	**ISO/IEC 27005 Indirect Operational Impacts**
Competitive Advantage – Losses associated with diminished competitive advantage. CA loss is specifically associated with assets that provide competitive differentiation between the organization and its competition. Examples include trade secrets, merger and acquisition plans, etc.	Opportunity cost (financial resources needed to replace or repair an asset would have been used elsewhere).
Fines/Judgments – Legal or regulatory actions levied against an organization. Note that this includes bail for any organization members who are arrested.	The cost of interrupted operations.
Reputation – Losses associated with an external perception that an organization’s value proposition is reduced or leadership is incompetent, criminal, or unethical.	Potential misuse of information obtained through a security breach.
	Violation of statutory or regulatory obligations.
	Violation of ethical codes of conduct.

3.5.5 Probability of Indirect Operational Impacts

In FAIR analysis, the probability of a primary loss event and the losses we can attribute to that event actually drive the probability of a secondary loss event. An organization actually has the opportunity to implement controls that will resist “threats” from identifiable sources of these secondary losses. For example, a primary incident concerning regulated information carries some probability of a second incident where government regulators are a new “threat source”. Past audits and other evidence of diligence may serve to help the organization resist (or limit) the force the regulators might apply (their fines).

So, in utilizing a FAIR approach to ISO/IEC 27005 loss estimation would be:

1. Identify direct operational impacts
2. Identify the source of secondary operational impacts
3. Perform subsequent analysis (as warranted) to determine the likelihood and impact of secondary operational impacts

3.6 Vulnerability Landscape

3.6.1 ISO Definition and Goal:

ISO/IEC 27005 §8.2.1.5 describes a need to identify vulnerabilities that can be exploited by threats to cause harm to assets. The outcome of §8.2.1.5 is a list of system or process weaknesses.

3.6.2 Major Differences in Vulnerability Landscape Treatment

There is no “vulnerability landscape” in Figure 4; rather the concept of “vulnerable” describes the information that is represented by where the threat, controls, and asset landscapes intersect. This is because, in FAIR, vulnerability describes knowledge about those landscapes, rather than a specific state of nature concerning system integrity. As such, in FAIR, vulnerability is derived as an outcome of the difference between control strength and threat capability. So in FAIR, if a threat’s capabilities are greater than the ability to resist, we have a significant degree of vulnerability. If, on the other hand, the ability to resist is greater than the threat’s capability, we are significantly less vulnerable.

In contrast, ISO treats vulnerabilities as system or process weaknesses in a system.

3.6.3 Consideration for the Vulnerability Landscape

In considering vulnerability, creating a list of system or process weaknesses is useful information to be gathered for the development of a FAIR control strength estimate. Analysts, however, are encouraged to think about vulnerability as a spectrum to describe the inherent uncertainty concerning the quality of threat landscape information.

3.6.4 Development of Metrics for the Vulnerability Landscape

As mentioned earlier, vulnerability in FAIR is a derived value that describes knowledge about the threat landscape and the controls landscape. The means to arrive at a vulnerability estimate is included later in this document.

4 How to use FAIR in your ISMS

The Information Security Management System (ISMS) is fundamentally a process, composed of tasks that transform input information into desired outputs. Thus, a task cannot be performed before all of its required inputs are available. FAIR decomposes the calculation of risk into its components, which constrains the precedence for task sequence. A third influence on task sequence is the series of one-to-many relationships among the data elements found in FAIR.

The following diagram depicts those relationships.

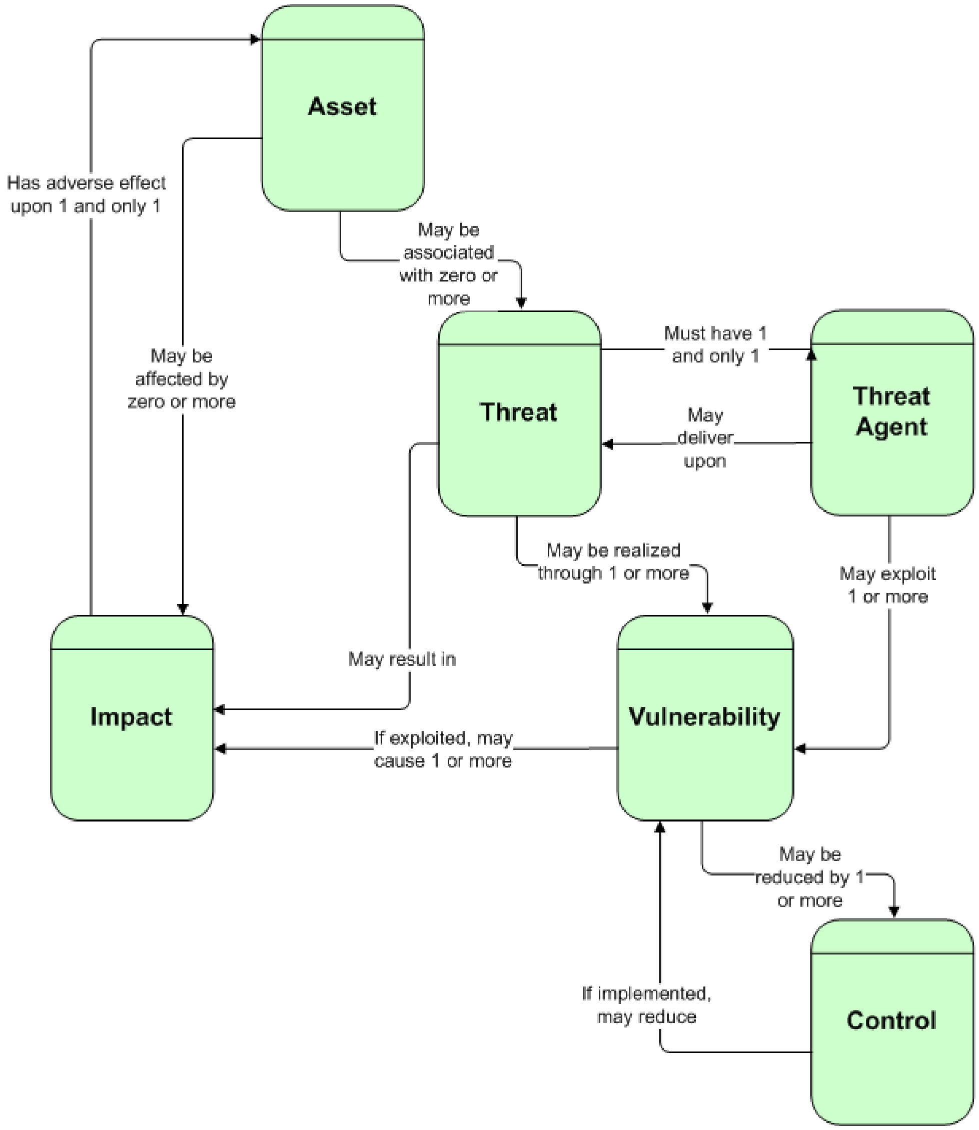

Asset
Has adverse effect upon 1 and only 1
May be associated with zero or more
May be affected by zero or more
Threat
Must have 1 and only 1
Threat Agent
May deliver upon
May be realized through 1 or more
May exploit 1 or more
May result in
Impact
If exploited, may cause 1 or more
Vulnerability
May be reduced by 1 or more
If implemented, may reduce
Control

Figure 5: ISMS Component Relationships

4.1 Recipe for ISO/IEC 27005 Risk Management with FAIR

This section presents the process for risk management, focusing on the inputs, actions, and outputs. You will see the sequence of steps that was provided in Section 2. Key input data (identified with underscores) was discussed in detail in Section 3. And this section provides the detailed explanation for the actions. Most text is drawn from ISO, with FAIR concepts *presented in italics*.

Table 4: ISO Inputs, Required Actions, and Outputs and how they can be used in FAIR

Inputs	**Actions – ISO**	**Outputs**
7.0 Context Establishment		
7.1 General Considerations		
All information about the organization relevant to establish the information security risk management context.	Establish the context for information security risk management: • Setting the basic criteria necessary for information security risk management (7.2) • Defining the scope and boundaries (7.3) • Establishing an appropriate organization operating the information security risk management (7.4)	A1 Specification of basic risk evaluation criteria A2 Scope and boundaries for risk analysis

Inputs	**Actions – FAIR**	**Outputs**
STAGE 1: Identify Scenario Components		
Identify the asset at risk:		
A2 Scope and boundaries for risk analysis + List of constituents with owners, location, function, etc.	*1 Identify each asset (e.g., information, application, etc.) and scope the asset (e.g., enterprise, business unit, etc.)*	B1 List of assets to be risk-managed
Identify the threat community:		

Inputs	**Actions – FAIR**	**Outputs**
+ Information on threats, from reviewing incidents, asset owners, users, external threat catalogs, other sources	*2 For each asset, identify the threat agent (e.g., insiders such as employees, contract workers; outsiders such as spies, thieves, competitors)* *3 For each threat agent, define the action and identify the contact* *4 Record the title and description of the threat*	C1 List of threats, with identification of threat type and threat source *C2 Threat title and description*
STAGE 2: Estimate Loss Event Frequency (LEF)		
Estimate probable Threat Event Frequency (TEF):		
B1 List of assets to be risk-managed C1 List of threats, with identification of evidences of frequency	*5 Estimate the Threat Event Frequency (TEF)* *6 For each threat, identify vulnerabilities that could be exploited by the threat agent*	*C3 Threat Event Frequency (TEF)* E1 List of vulnerabilities in relation to assets, threats, and controls
Estimate Threat Capability (TCap):		
E1 List of vulnerabilities in relation to assets, threats, and controls	*7 Estimate the threat's capabilities relative to each vulnerability*	*E3 Threat capability*
Estimate Control Strength (CS):		
+ Documentation of controls + Documentation risk treatment implementation plans. *E3 Threat capability*	*9 For each vulnerability, identify existing controls that reduce the vulnerability* *10 Evaluate the control strength for each control*	D1 *Control Strength (CS) –* List of all existing and planned controls, their effectiveness, implementation, and usage status
Derive Vulnerability (Vuln):		
D1 *Control Strength (CS) –* List of all existing and planned controls, their effectiveness, implementation, and usage status	*11 Calculate Vulnerability (Vuln)*	*D2 Vulnerability (Vuln)*
Derive Loss Event Frequency (LEF):		
C3 Threat Event Frequency (TEF) D1 List of all existing and planned controls, their effectiveness, implementation, and usage status *D2 Vulnerability (Vuln)*	*12 Calculate Loss Event Frequency (LEF)*	*H2 Loss Event Frequency (LEF)*

Inputs	Actions – FAIR	Outputs
STAGE 3: Evaluate Probable Loss Magnitude (PLM)		
Estimate worst-case loss:		
Estimate Probable Loss Magnitude (PLM):		
C2 Threat title and description	*8 Estimate potential impacts for each threat*	*G2 Probable Loss Magnitude (PLM) for each threat*
STAGE 4: Derive and Articulate Risk		
A1 Specification of basic risk evaluation criteria *D2 Vulnerability (Vuln)* *H2 Loss Event Frequency (LEF)* *G2 Probable Loss Magnitude (PLM)*	*13 Calculate risk* *14 Produce risk reports*	*I1 Risk* J1 List of risks prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks *J2 Prioritized control improvements*

Inputs	Actions – ISO	Outputs
9.0 Information security risk treatment		
9.1 General description of risk treatment		
I1,J1 List of risks prioritized according to risk evaluation criteria in relation to the incident scenarios that lead to those risks	Select controls to reduce, retain, avoid, or transfer the risks Prepare a risk treatment plan	K1 Risk treatment plan K2 Residual risks subject to the acceptance decision of the organization's managers
9.2 Risk Reduction	Reduce risk by selecting controls so that the residual risk can be reassessed as being acceptable	
9.3 Risk Retention	Decide to retain the risk without further action, based on risk evaluation	
9.4 Risk Avoidance	Avoid the activity or condition that gives rise to the particular risk	
9.5 Risk Transfer	Transfer the risk to another party that can most effectively manage the particular risk, based on risk evaluation	

Inputs	Actions – ISO	Outputs
10.0 Information Security Risk Acceptance		
K1 Risk treatment plan K2 Residual risk assessment subject to the acceptance decision of the organization’s managers	The decision to accept the risks and responsibilities for the decision should be made and formally recorded (this relates to ISO/IEC 27001 §4.2.1 (h)).	List of accepted risks with justification for those that do not meet the organization’s normal risk acceptance criteria

Inputs	Actions – ISO	Outputs
11.0 Information Security Risk Communication		
All risk information obtained from the risk management activities	Information about risk should be exchanged and/or shared between the decision-maker and other stakeholders.	Continual understanding of the organization’s information security risk management process and results

Inputs	Actions – ISO	Outputs
12.0 Information Security Risk Monitoring and Review		
12.1 Monitoring and Review of Risk Factors		
All risk information obtained from the risk management activities	Monitor and review risks and their factors (i.e., value of assets, impacts, threats, vulnerabilities, likelihood of occurrence) to identify any changes in the context of the organization at an early stage, and to maintain an overview of the complete risk picture	Continual alignment of the management of risks with the organization’s business objectives, and with risk acceptance criteria
12.2 Risk Management Monitoring, Reviewing, and Improving		
All risk information obtained from the risk management activities		Continual relevance of the information security risk management process to the organization’s business objectives or updating the process

4.2 Define the Context for Information Risk Management

4.2.1 General Considerations

Establish the context for information security risk management:

- Setting the basic criteria necessary for information security risk management (ISO/IEC 27005 §7.2)
- Defining the scope and boundaries (ISO/IEC 27005 §7.3)
- Establishing an appropriate organization operating the information security risk management (ISO/IEC 27005 §7.4)

The organization must have the resources to appropriately engage in a risk management process. These resources must include the following:

- Perform risk assessments
- Develop risk treatment plans
- Define and implement policies and procedures to implement selected controls
- Monitor implemented controls
- Monitor the overall risk management process

Without such resources, establishing a risk management process will set expectations of the organization that cannot be met.

This task should be performed from an organizational perspective for the overall development of the ISMS, but also considered for each risk assessment to ensure success of the risk assessment results.

4.2.2 Risk Acceptance Criteria

Developing a set of risk acceptance criteria based on the goals and objectives of the organization is important to have as an integral part of the ISMS. This assists in the development of risk treatment plans. Developing a list of risk acceptance criteria sets the groundwork for determining what risks the organization is capable of accepting, in general terms. This is probably done once when developing the ISMS, but may need to be adjusted for each risk assessment performed at the time of risk treatment plan development.

Risk acceptance criteria should be developed and specified. Risk acceptance criteria often depend on the organization's policies, goals, objectives, and the interests of stakeholders.

An organization should define its own scales for levels of risk acceptance. The following should be considered during development:

- Risk acceptance criteria may include multiple thresholds, with a desired target level of risk, but provision for senior managers to accept risks above this level under defined circumstances.

- Risk acceptance criteria may be expressed as the ratio of estimated profit (or other business benefit) to the estimated risk.
- Different risk acceptance criteria may apply to different classes of risk; e.g., risks that could result in non-compliance with regulations or laws may not be accepted, while acceptance of high risks may be allowed if this is specified as a contractual requirement.
- Risk acceptance criteria may include requirements for future additional treatment; e.g., a risk may be accepted if there is approval and commitment to take action to reduce it to an acceptable level within a defined time period.
- Risk acceptance criteria may differ according to how long the risk is expected to exist; e.g., the risk may be associated with a temporary or short-term activity.

In developing the risk acceptance criteria, the following should be considered:

- Business criteria
- Legal and regulatory aspects
- Operational considerations
- Technological aspects
- Financial considerations
- Social and humanitarian factors

Place the organization's generalized risk acceptance criteria from the ISMS in Question 2 of the Risk Management Program Worksheet (Appendix A).

Consider whether there are specific risk acceptance criteria for the risk assessment under consideration in Question 3 of the Risk Management Program Worksheet (Appendix A).

4.3 Calculate Risk

4.3.1 Stage 1

Identify each asset (e.g., information, application, etc.) and scope the asset (e.g., enterprise, business unit, etc.).

Describe the Asset(s) and Critical Attributes under Consideration

Identification and description of the assets under consideration during a risk assessment is critical. Identify the asset(s) under consideration during this risk assessment in Question 3 of the Risk Management Program Worksheet (Appendix A).

Describe the Threat(s) to the Asset(s) under Consideration

For each asset, identify the threat agent(s) (e.g., insiders such as employees, contract workers; outsiders such as spies, thieves, competitors) in the space provided in Question 4 of the Risk Management Program Worksheet (Appendix A).

For each threat agent describe the frequency with which threat agents may come into contact with the asset(s) under consideration in the space provided in Question 4 of the Risk Management Program Worksheet (Appendix A).

For each threat agent, estimate the probability that they will act against the asset(s) in the space provided in Question 4 of the Risk Management Program Worksheet (Appendix A).

Define the potential action and describe the threat(s) in the space provided in Question 4 of the Risk Management Program Worksheet (Appendix A).

4.3.2 Stage 2

Estimate the Loss Event Frequency (LEF).

The Loss Event Frequency (LEF) considers the following factors: Threat Event Frequency (TEF), Threat Capability (TCap), Control Strength (CS), and Vulnerability (Vuln).

Estimate the Probable Threat Event Frequency (TEF)

Estimate the probable Threat Event Frequency (TEF). Use the information in Question 4 of the Risk Management Program Worksheet (Appendix A).

The following table shows the ratings for the values of the Threat Event Frequency (TEF). Circle the estimated Threat Event Frequency (TEF) in Question 5 of the Risk Management Program Worksheet (Appendix A).

Rating	Description
Very High (VH)	> 100 times per year
High (H)	Between 10 and 100 times per year
Moderate (M)	Between 1 and 10 times per year
Low (L)	Between 0.1 and 1 times per year
Very Low (VL)	< 0.1 times per year (less than once every 10 years)

Estimate the Threat Capability (TCap)

Estimate the Threat Capability (TCap), which is the capability that the threat community has to act against the asset using a specific threat. Use the information in Question 4 of the Risk Management Program Worksheet (Appendix A).

The following table shows the ratings for the values of Threat Capability (TCap). Circle the Threat Capability (TCap) in Question 6 of the Risk Management Program Worksheet (Appendix A).

Rating	Description
Very High (VH)	Top 2% when compared against the overall threat population
High (H)	Top 16% when compared against the overall threat population
Moderate (M)	Average skill and resources (between bottom 16% and top 16%)
Low (L)	Bottom 16% when compared against the overall threat population
Very Low (VL)	Bottom 2% when compared against the overall threat population

Estimate the Control Strength (CS)

Estimate the Control Strength (CS), which represents the probability that the organization’s controls will be able to withstand a baseline measure of force. Use the information in Question 4 of the Risk Management Program Worksheet (Appendix A).

The following table shows the ratings for the values of Control Strength (CS).

Rating	Description
Very High (VH)	Protects against all but the top 2% of an average threat population
High (H)	Protects against all but the top 16% of an average threat population
Moderate (M)	Protects against the average threat agent
Low (L)	Only protects against bottom 16% of an average threat population
Very Low (VL)	Only protects against bottom 2% of an average threat population

Derive the Vulnerability (Vuln)

Derive the Vulnerability (Vuln) using the vulnerability matrix below. Locate the intersection of Threat Capability (TCap) and Control Strength (CS) from Question 6 and 7 of the Risk Management Program Worksheet (Appendix A). Circle the Vulnerability (Vuln) in Question 8 of the Risk Management Program Worksheet (Appendix A).

Vulnerability (Vuln)

		VL	L	M	H	VH
Threat Capability (TCap)	**VH**	VH	VH	VH	H	M
	H	VH	VH	H	M	L
	M	VH	H	M	L	VL
	L	H	M	L	VL	VL
	VL	M	L	VL	VL	VL

Control Strength (CS)

Derive Loss Event Frequency (LEF)

Derive the Loss Event Frequency (LEF) using the Loss Event Frequency (LEF) matrix below. Locate the intersection of Threat Event Frequency (TEF) and Vulnerability (Vuln) to derive Loss Event Frequency (LEF) from Question 5 and 8 of the Risk Management Program Worksheet (Appendix A). Circle the Loss Event Frequency (LEF) in Question 9 of the Risk Management Program Worksheet (Appendix A).

Loss Event Frequency (LEF)

	VH	M	H	VH	VH	VH
Threat Event Frequency (TEF)	**H**	L	M	H	H	H
	M	**VL**	**L**	M	M	M
	L	**VL**	VL	L	L	L
	VL	VL	VL	VL	VL	VL
		VL	**L**	**M**	**H**	**VH**

Vulnerability (Vuln)

4.3.3 Stage 3

Evaluate the Probable Loss Magnitude (PLM).

Determine the probable impact of the loss. This is identified as the Probable Loss Magnitude (PLM). This includes estimating the worst-case scenario as well as the most probable scenario(s) of loss.

Estimate the Worst-Case Loss and Probable Loss Magnitude (PLM)

Use the following values to determine the magnitudes for the worst-case scenarios and Probably Loss Magnitude (PLM) for each appropriate threat action and loss form. The range values should be adjusted appropriately to meet the needs of the organization.

Magnitude	**Range Low End**	**Range High End**
Severe (SV)	$10,000,000	–
High (H)	$1,000,000	$9,999,999
Significant (Sg)	$100,000	$999,999
Moderate (M)	$10,000	$99,999
Low (L)	$1,000	$9,999
Very Low (VL)	$0	$999

For each threat action, enter the magnitude into the tables in Question 10 and 11 of the Risk Management Program Worksheet (Appendix A).

4.3.4 Stage 4

Derive and articulate risk.

Derive the Risk Magnitude

Once we have estimates of Loss Event Frequency (LEF) and Probable Loss Magnitude (PLM), we are able to derive the risk value from the risk matrix below.

The following matrix is used to derive risk using Probable Loss Magnitude (PLM) and Loss Event Frequency (LEF). Identify the intersection of the Probable Loss Magnitude (PLM) and Loss Event Frequency (LEF) from Question 9 and 11 of the Risk Management Program Worksheet (Appendix A). Circle the Risk in Question 12 of the Risk Management Program Worksheet (Appendix A).

Risk

Probable Loss Magnitude (PLM)	**Severe**	H	H	C	C	C
	High	M	H	H	C	C
	Significant	M	M	H	H	C
	Moderate	L	M	M	H	H
	Low	L	L	M	M	M
	Very Low	L	L	M	M	M
		VL	**L**	**M**	**H**	**VH**

Loss Event Frequency (LEF)

Key for Risk Values

Key	**Risk Level**
C	Critical
H	High
M	Moderate
L	Low

Articulate the Real Risk

The real challenge has to do with articulating this risk value to the decision-makers. This can be performed using the information gathered through this entire process using the ISO/IEC 27005 communication framework.

A major consideration of communicating risk levels is the association of qualitative labeling with a tendency to equate “high-risk” with “unacceptable”, and “low-risk” with “acceptable”. In fact, in some circumstances high-risk is entirely acceptable (e.g., in cases where the potential for reward outweighs the risk). In other situations, a relatively low-risk condition may be unacceptable, particularly if the exposure is systemic within an organization. Including more specific information regarding Loss Event Frequency (LEF) and Probable Loss Magnitude (PLM) can help to reduce the bias associated with qualitative risk labels.

In summary, risk articulation must meet the needs of the decision-makers. When using qualitative labels for range values, it is imperative to ensure that management agrees with the criteria for each range/level.

4.4 Determine the Appropriate Information Risk Treatment Plan

The four options available for risk treatment are:

- **Risk Reduction** – Actions taken to lessen the probability, negative consequences, or both, associated with a risk.
- **Risk Avoidance –** Decision not to become involved in, or action to withdraw from, a risk situation.
- **Risk Transfer** – Sharing with another party the burden of loss or benefit of gain, for a risk.
- **Risk Retention** – Acceptance of the burden of loss or benefit of gain from a particular risk.

The four options for risk treatment are not mutually-exclusive. Sometimes the organization can benefit substantially by a combination of options.

Some risk treatments can effectively address more than one risk. A risk treatment plan should be defined which clearly identifies the priority ordering in which individual risk treatments should be implemented and their timeframes.

Using the determination of risk magnitude and the discussion of actual risk from Question 12 and 13 of the Risk Management Program Worksheet (Appendix A) and the Generalized Risk Acceptance Criteria in Question 2 of the Risk Management Program Worksheet (Appendix A), answer the question in Question 14 of the Risk Management Program Worksheet (Appendix A).

Using the information provided in Question 2 of the Risk Management Program Worksheet (Appendix A), assess whether the risk will be at an acceptable level for the organization once the treatment plan has been implemented. Circle the appropriate answer in Question 15 of the Risk Management Program Worksheet (Appendix A).

4.5 Develop an Information Security Risk Communication Plan

The steps involved in risk communication is a bi-directional process designed to achieve agreement on how to manage risks by exchanging and/or sharing information about risk between the decision-makers and other stakeholders.

Effective communication among stakeholders is important since this may have a significant impact on decisions that must be made. Communication will ensure that those responsible for implementing risk management, and those with a vested interest, understand the basis on which decisions are made and why particular actions are required.

Perceptions of risk can vary due to differences in assumptions, concepts, and the needs, issues, and concerns of stakeholders as they relate to risk or the issues under discussion. Stakeholders are likely to make judgments on the acceptability of risk based on their perception of risk. This is especially important to ensure that the stakeholders' perceptions of risk, as well as their perceptions of benefits, can be identified and documented and the underlying reasons clearly understood and addressed.

Using all of the information gathered in the Risk Management Program Worksheet (Appendix A) as input, answer the items in Question 16 of the Risk Management Program Worksheet (Appendix A).

4.6 Describe the Information Security Risk Monitoring and Review Plan

Risks are not static. Threats, vulnerabilities, likelihood, or consequences may change abruptly without any indication. Therefore, constant monitoring is necessary to detect these changes.

Organizations should ensure that the following are continually monitored:

- 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 inside and outside the organization and that have not been assessed
- 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
- Information security incidents

New threats, vulnerabilities, or changes in probability or consequences can increase risks previously assessed as low. Review of low and accepted risks should consider each risk separately, and all such risks as an aggregate as well, to assess their potential accumulated impact if risks do not fall into the low or acceptable risk category.

Answer the items in Question 17 of the Risk Management Program Worksheet (Appendix A).

A Risk Management Program Worksheet

A.1 Define the Context for Information Risk Management

General Considerations

1. Are the following resources available in the organization to support the risk management program?

Are resources available to conduct risk assessments? Yes No

Describe these resources below:

Are resources available to develop risk treatment plans? Yes No

Describe these resources below:

Are resources available to implement the selected controls? Yes No

Describe these resources below:

Are resources available to establish policies and procedures to support the selected controls? Yes No

Describe these resources below:

Are resources available to monitor the implemented controls? Yes No

Describe these resources below:

Are resources available to monitor the overall risk management program? Yes No

Describe these resources below:

2. What are the organization’s generalized risk acceptance criteria from the ISMS?

Are adjustments to the organizations risk acceptance criteria necessary? Yes No

If yes, define the adjustments below:

A.2 Calculate Risk

Stage 1: Identify Scenario Components of Asset(s) and Threat(s)

Identify each asset(s) (e.g., information, application, etc.) and scope the asset(s) (e.g., enterprise, business unit, etc.).

3. Describe the asset(s) under consideration:

Identify the Threat Community

4. Identify the threats that can impact the asset(s).

Describe the potential threat agents:

Describe the potential frequency with which threat agents may come into contact the asset(s):

Probability that threat agents will act against the asset(s):

Define the anticipated actions and describe the potential threat(s):

Stage 2: Evaluate Loss Event Frequency (LEF)

5. Estimate the probable Threat Event Frequency (TEF). Select the rating below:

Very High (VH) High (H) Moderate (M) Low (L) Very Low (VL)

6. Estimate the probable Threat Capability (TCap). Select the rating below:

Very High (VH) High (H) Moderate (M) Low (L) Very Low (VL)

7. Identify existing and planned controls:

Describe controls:

Estimate the Control Strength (CS) for the control state. Select the rating below:

Very High (VH) High (H) Moderate (M) Low (L) Very Low (VL)

8. Derive the Vulnerability (Vuln) Level. Select the rating below:

Very High (VH) High (H) Moderate (M) Low (L) Very Low (VL)

9. Derive Loss Event Frequency (LEF). Select the rating below:

Very High (VH) High (H) Moderate (M) Low (L) Very Low (VL)

Stage 3: Evaluate Probable Loss Magnitude (PLM)

10. Estimate worst-case loss:

	Loss Forms					
Threat Action	**Productivity**	**Response**	**Replace-ment**	**Fine Judgments**	**Competitive Advantage**	**Reputation**
Access						
Misuse						
Disclosure						
Modification						
Deny Access						

11. Estimate Probable Loss Magnitude (PLM):

	Loss Forms					
Threat Action	**Productivity**	**Response**	**Replace-ment**	**Fine Judgments**	**Competitive Advantage**	**Reputation**
Access						
Misuse						
Disclosure						
Modification						
Deny Access						

Stage 4: Derive and Articulate Risk

12. Derive the risk level. Select the risk magnitude below:

Critical (C) High (H) Moderate (M) Low (L)

13. Articulate and discuss the risk below:

A.3 Determine the Appropriate Information Risk Treatment Plan

14. Define the Information Risk Treatment Plan.

Risk Reduction Methods

What actions will be taken to reduce the risks associated with the identified threats on the associated assets(s)?

What are the expected costs of these risk reduction activities?

What are the expected benefits of these risk reduction activities?

Risk Avoidance Methods

Based on the identified risks, will the organization avoid these risks by either withdrawing from this activity or discontinue participating in this activity? Yes No

What are the expected costs or losses to the organization of avoiding this risk?

What are the expected benefits to the organization of avoiding this risk?

Risk Transfer Options

Describe the available options for transferring all or parts of the identified risks:

What are the expected costs of the identified risk transfer options?

What are the expected benefits of the identified risk transfer options?

Risk Retention

Describe the risks that will be retained by the organization:

15. Is the risk at acceptable level? Yes No

A.4 Develop an Information Security Risk Communication Plan

16. Develop the Information Security Risk Communication Plan.

Who are the stakeholders that are required to approve the risk treatment plan?

Who are the decision-makers that are required to approve the risk treatment plan?

Describe the methods that will be used to communicate the risks to the identified stakeholders and decision-makers (i.e., risk reports, presentation, etc.):

Describe the documentation expected from the decision-makers to approve the risk treatment plan:

A.5 Describe the Information Security Risk Monitoring and Review Plan

17. Risk monitoring and review for the identified asset(s), threats(s), and vulnerabilities(s).

Describe the available resources and/or systems in place to monitor the risks, threats, and vulnerabilities identified through this process:

Describe how the change management process within the organization will be used to monitor assets included in this assessment:

Glossary

Term	Source	ISO/FAIR Definition
Action	FAIR	An act taken against an asset by a threat agent. Requires first that contact occur between the asset and threat agent.
Activity	ISO/IEC 27005	Used synonymously with Process.
Asset	FAIR	Any data, device, or other component of the environment that supports information-related activities, which can be illicitly accessed, used, disclosed, altered, destroyed, and/or stolen, resulting in loss.
	ISO/IEC 27001 ISO/IEC 27002	Anything that has value to the organization.
Asset Factors	FAIR	See Factors, Asset.
Availability	ISO/IEC 27001	The property of being accessible and usable upon demand by an authorized entity.
Broad Spectrum Risk Analysis	FAIR	See Risk Analysis, Broad Spectrum.
Confidentiality	ISO/IEC 27001	The property that information is not made available or disclosed to unauthorized individuals, entities, or processes.
Contact	FAIR	Occurs when a threat agent establishes a physical or virtual (e.g., network) connection to an asset.
Contact Frequency	FAIR	The probable frequency, within a given timeframe, that a threat agent will come into contact with an asset.
Control	ISO/IEC 27002	Means of managing risk, including policies, procedures, guidelines, practices, or organizational structures, which can be of administrative, technical, management, or legal nature. NOTE: Control is also used as a synonym for safeguard or countermeasure.
Control Strength	FAIR	The strength of a control as compared to a baseline measure of force.
Environmental Factors	FAIR	See Factors, Environmental.
Factors, Asset	FAIR	Characteristics of the asset(s) that drive loss magnitude.

Term	Source	ISO/FAIR Definition
Factors, Environmental	FAIR	Characteristics of the environment in which the organization operates that drive loss magnitude.
Frequency, Loss Event	FAIR	The probable frequency, within a given timeframe, that a threat agent will inflict harm upon an asset.
Frequency, Threat Event	FAIR	The probable frequency, within a given timeframe, that a threat agent will act against an asset.
Guideline	ISO/IEC 27002	A description that clarifies what should be done and how, to achieve the objectives set out in policies..
Impact	ISO/IEC 27005	Adverse change to the level of business objectives achieved
Information Security	ISO/IEC 27001 ISO/IEC 27002	Preservation of confidentiality, integrity, and availability of information; in addition, other properties, such as authenticity, accountability, non-repudiation, and reliability can also be involved.
Information Security Event	ISO/IEC 27001 ISO/IEC 27002	An identified occurrence of a system, service, or network state indicating a possible breach of information security policy or failure of safeguards, or a previously unknown situation that may be security relevant.
Information Security Incident	ISO/IEC 27001 ISO/IEC 27002	An information security incident is indicated by a single or a series of unwanted or unexpected information security events that have a significant probability of compromising business operations and threatening information security.
Information Security Management System (ISMS)	ISO/IEC 27001	That part of the overall management system, based on a business risk approach, to establish, implement, operate, monitor, review, maintain and improve information security.
Information Security Risk	ISO/IEC 27005	See Risk, Information Security.
Integrity	ISO/IEC 27001	The property of safeguarding the accuracy and completeness of assets.
Likelihood	ISO/IEC 27005	Used synonymously with Probability.
Loss Event	FAIR	A loss event occurs when a threat agent’s action (threat event) is successful in negatively affecting an asset.
Loss Event Frequency	FAIR	See Frequency, Loss Event.
Loss Factors, Primary	FAIR	Factors that drive loss magnitude based solely on the nature of the asset and the threat agent’s action.

Term	Source	ISO/FAIR Definition
Loss Factors, Secondary	FAIR	Factors that drive loss magnitude based on organizational and environmental conditions.
Method	FAIR	A rule or orderly procedure used in carrying out a task or accomplishing an aim.
Methodology	FAIR	A system of methods and rules applied to work on a given subject.
Multilevel Risk Analysis	FAIR	See Risk Analysis, Multilevel.
Organizational Factors	FAIR	Characteristics of the organization that drive loss magnitude.
Policy	ISO/IEC 27002	Overall intention and direction as formally expressed by management.
Primary Loss Factors	FAIR	See Loss Factors, Primary.
Probability of Action	FAIR	The probability that a threat agent will act against an asset once contact has occurred.
Probable Loss Magnitude	FAIR	The probable magnitude of loss resulting from threat agent's action.
Residual Risk	ISO/IEC 27001	See Risk, Residual.
Risk	FAIR	The probable frequency and probable magnitude of future loss.
	ISO/IEC 27002	Combination of the probability of an event and its consequence.
Risk, Derived	FAIR	Risk that is derived from the risk matrix using Probable Loss Magnitude (PLM) and Loss Event Frequency (LEF).
Risk, Information Security	ISO/IEC 27005	Potential that a given threat will exploit vulnerabilities of an asset or group of assets and thereby cause harm to the organization. NOTE: It is measured in terms of a combination of the likelihood of an event and its consequence.
Risk, Residual	ISO/IEC 27001	The risk remaining after risk treatment.
Risk Acceptance	ISO/IEC 27001	Decision to accept a risk.
Risk Analysis	ISO/IEC 27001 ISO/IEC 27002	Systematic use of information to identify sources and to estimate the risk.
Risk Analysis, Broad Spectrum	FAIR	Any analysis that accounts for the risk from multiple threat communities against a single asset.

Term	Source	ISO/FAIR Definition
Risk Analysis, Multilevel	FAIR	Any analysis that accounts for the risk from a single threat community against a layered set of assets (e.g., defense in-depth).
Risk Assessment	ISO/IEC 27001 ISO/IEC 27002	Overall process of risk analysis and risk evaluation.
Risk Avoidance	ISO/IEC 27005	Decision not to become involved in, or action to withdraw from, a risk situation.
Risk Communication	ISO/IEC 27005	Exchange or sharing of information about risk between the decision-maker and other stakeholders.
Risk Estimation	ISO/IEC 27005	Process to assign values to the probability and consequences of a risk.
Risk Evaluation	ISO/IEC 27001 ISO/IEC 27002	Process of comparing the estimated risk against given risk criteria to determine the significance of the risk.
Risk Identification	ISO/IEC 27005	Process to find, list, and characterize elements of risk.
Risk Management	ISO/IEC 27001 ISO/IEC 27002	Coordinated activities to direct and control an organization with regard to risk. NOTE: Risk management typically includes risk assessment, risk treatment, risk acceptance, and risk communication.
Risk Reduction	ISO/IEC 27005	Actions taken to lessen the probability, negative consequences, or both, associated with a risk.
Risk Retention	ISO/IEC 27005	Acceptance of the burden of loss or benefit of gain from a particular risk.
Risk Transfer	ISO/IEC 27005	Sharing with another party the burden of loss or benefit of gain, for a risk.
Risk Treatment	ISO/IEC 27001 ISO/IEC 27002	Process of selection and implementation of measures to modify risk.
Secondary Loss Factors	FAIR	See Loss Factors, Secondary.
Taxonomy	FAIR	A systematic description of the subcomponents and their relationships within a complex subject.
Threat	FAIR	Anything that is capable of acting in a manner resulting in harm to an asset and/or organization; for example, acts of God (weather, geological events, etc.), malicious actors, errors, failures.
	ISO/IEC 27002	A potential cause of an unwanted incident, which may result in harm to a system or organization.

Term	**Source**	**ISO/FAIR Definition**
Threat Agent	FAIR	Any agent (e.g., object, substance, human, etc.) that is capable of acting against an asset in a manner that can result in harm.
Threat Capability	FAIR	The probable level of force that a threat agent is capable of applying against an asset.
Threat Community	FAIR	A subset of the overall threat agent population that shares key characteristics.
Threat Event	FAIR	The probable frequency, within a given timeframe, that a threat agent will act against an asset.
Threat Event Frequency	FAIR	See Frequency, Threat Event.
Threat Factors	FAIR	Characteristics of the threat agent that drive loss magnitude.
Vulnerability	FAIR	The probability that an asset will be unable to resist actions of a threat agent.
	ISO/IEC 27002	A weakness of an asset or group of assets that can be exploited by one or more threats.
Vulnerability, Derived	FAIR	Vulnerability (Vuln) derived from the vulnerability matrix using Threat Capability (TCap) and Control Strength (CS).

Index