ISO27001:2022
Lec2

History of 27001

what is information security ?

ISO 27001 INFORMATION SECURITY MANAGEMENT SYSTEM

Confidentiality

Maintaining confidentiality is important to ensure that sensitive information doesn't end up in the hands of the wrong people. In order to do this, access must be restricted to only authorized individuals. Some methods that could be used to protect confidentiality include encryption, two-factor authentication, unique user IDs, strong passwords, etc.

Integrity

Maintaining the integrity of sensitive data means maintaining its accuracy and authenticity of the data. This means that sensitive data must be protected from accidental or intentional changes that could taint the data. File permissions and access controls are just a couple of things that can be implemented to help protect integrity.

Availability

Maintaining availability means that your services, information, or other critical assets are available to your customers when needed.
This doesn't just apply to lost or destroyed data, but also when access is delayed. Developing a disaster recovery plan and performing regular backups are some ways to help maintain availability of critical assets.

Structure of ISO27001 – Clauses (4 - 10)

1) Introduction & general overview of standard.

2) Scope of the standards Applicable to all types of organizations

3) Definitions

4) Context of the organization

5) Leadership & Top Management

6) Planning

7) Support – Availability of resources

8) Operation

9) Performance

10) Improvement

Understanding of the Organization

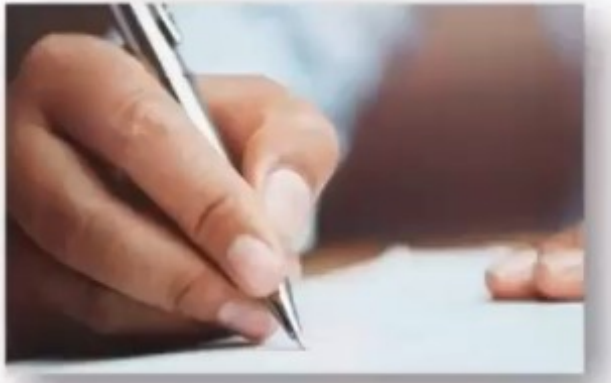
Context of the Organization - ISO/IEC 27001, clauses 4.1 and 4.2

4.1 Understanding the organization and its context

context means environment in which the organization seeks to achieve its objectives

The organization shall determine external and internal issues that are relevant to its purpose and that affect its ability to achieve the intended outcome(s) of its information security management system.

- Determine legal and regulatory requirements, stakeholder perceptions , social and cultural, political, financial, technological, economic, natural and competitive environment, whether international, national, regional or local.
- key drivers and trends having impact on the objectives of the organization
- Relationships with, perceptions and values of external stakeholders.



Understanding of the Organization – Continued

Context of the Organization - ISO/IEC 27001, clauses 4.1 and 4.2

4.1 Understanding the organization and its context

- An organization wishing to comply with ISO/IEC 27001 shall at least:

1. Be able to demonstrate that its ISMS is aligned with its mission, its objectives and business strategies;
2. Identify and document the organization's activities, functions, services, products, partnerships, supply chains and relationships with interested parties;
3. Define the external and internal factors that can influence the ISMS;
4. Recognize and take into account issues related to information security within their industrial sector such as risk, legal and regulatory obligations and customer requirements.
5. Establish and document objectives for the ISMS.

- **External issues** are those outside of the organization's control. This is often referred to as the organization's environment. Analysing this environment can include the following aspects: social and cultural; political, legal, normative and regulatory; financial and macroeconomic; technological; natural; and competitive.
- **Internal issues** are subject to the organization's control. Analysing the internal issues can include the following aspects: the organization's culture; policies, objectives, and the strategies to achieve them; governance, organizational structure, roles and responsibilities; standards, guidelines and models adopted by the organization; contractual relationships that can directly affect the organization's processes included in the scope of the ISMS; processes and procedures; the capabilities, in terms of resources and knowledge (e.g. capital, time, persons, processes, systems and technologies); physical infrastructure and environment; information systems,

Understanding of the Organization – Continued

4.1 Understanding the organization and its context

Tasks to do

- **Understanding of the mission, objectives, values, strategies of the organization**
- Analyzing the external environment
- Analyzing the internal environment
- Identification of the key processes and activities
- Identification of the infrastructure
- Identification and analysis of interested parties
- Determination of the ISMS objectives
- Preliminary definition of the scope

Result

- Brief description of the organization and its environment
- List of stakeholders and their requirements
- List of applicable legal, regulatory and contractual obligations
- Objectives and priorities related to ISMS
- Preliminary Scope

Understanding of the Organization – Continued

4.1 Understanding the organization and its context

Tasks to do

- Understanding of the mission, objectives, values, strategies of the organization
- **Analyzing the external environment**
- **Analyzing the internal environment**
- Identification of the key processes and activities
- Identification of the infrastructure
- Identification and analysis of interested parties
- Preliminary definition of the scope

Result

- Brief description of the organization and its environment
- List of stakeholders and their requirements
- List of applicable legal, regulatory and contractual obligations
- Objectives and priorities related to ISMS
- Preliminary Scope

Understanding of the Organization – Continued

4.1 Understanding the organization and its context

Tasks to do

- Understanding of the mission, objectives, values, strategies of the organization
- Analyzing the external environment
- Analyzing the internal environment
- Identification of the key processes and activities
- Identification of the infrastructure
- Identification and analysis of interested parties
- Preliminary definition of the scope

Result

- Brief description of the organization and its environment
- List of stakeholders and their requirements
- List of applicable legal, regulatory and contractual obligations
- Objectives and priorities related to ISMS
- Preliminary Scope

Understand:
- Goods and services produced by the organization
- Business Processes
- Information assets

Understanding of the Organization – Continued

4.1 Understanding the organization and its context

Tasks to do

- Understanding of the mission, objectives, values, strategies of the organization
- Analyzing the external environment
- Analyzing the internal environment
- Identification of the key processes and activities
- **Identification of the infrastructure**
- Identification and analysis of interested parties
- Preliminary definition of the scope

Result

- Brief description of the organization and its environment
- List of stakeholders and their requirements
- List of applicable legal, regulatory and contractual obligations
- Objectives and priorities related to ISMS
- Preliminary Scope

Hardware, Software, Networks, Sites

4 - Context of the Organization

Context of the Organization - ISO/IEC 27001, clauses 4.2

4.2 Understanding the needs and expectations of interested parties

The organization shall determine
a. interested parties that are relevant to the information security management system; and
b. the requirements of these interested parties relevant to information security.

Tasks to do

- Understanding of the mission, objectives, values, strategies of the organization
- Analyzing the external environment
- Analyzing the internal environment
- Identification of the key processes and activities
- Identification of the infrastructure
- **Identification and analysis of interested parties**
- Preliminary definition of the scope

Result

- Brief description of the organization and its environment
- List of stakeholders and their requirements
- List of applicable legal, regulatory and contractual obligations
- Objectives and priorities related to ISMS
- Preliminary Scope

- Identify all interested parties and their requirements and expectations and involve them in ISMS project

Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

4.3 Determining the scope of the information security management system

The organization shall determine the boundaries and applicability of the information security management system to establish its scope. When determining this scope, the organization shall consider:

a. the external and internal issues referred to in 4.1;
b. the requirements referred to in 4.2; and
c. interfaces and dependencies between activities performed by the organization, and those that are performed by other organizations.

Why we need to approve the ISMS Scope?

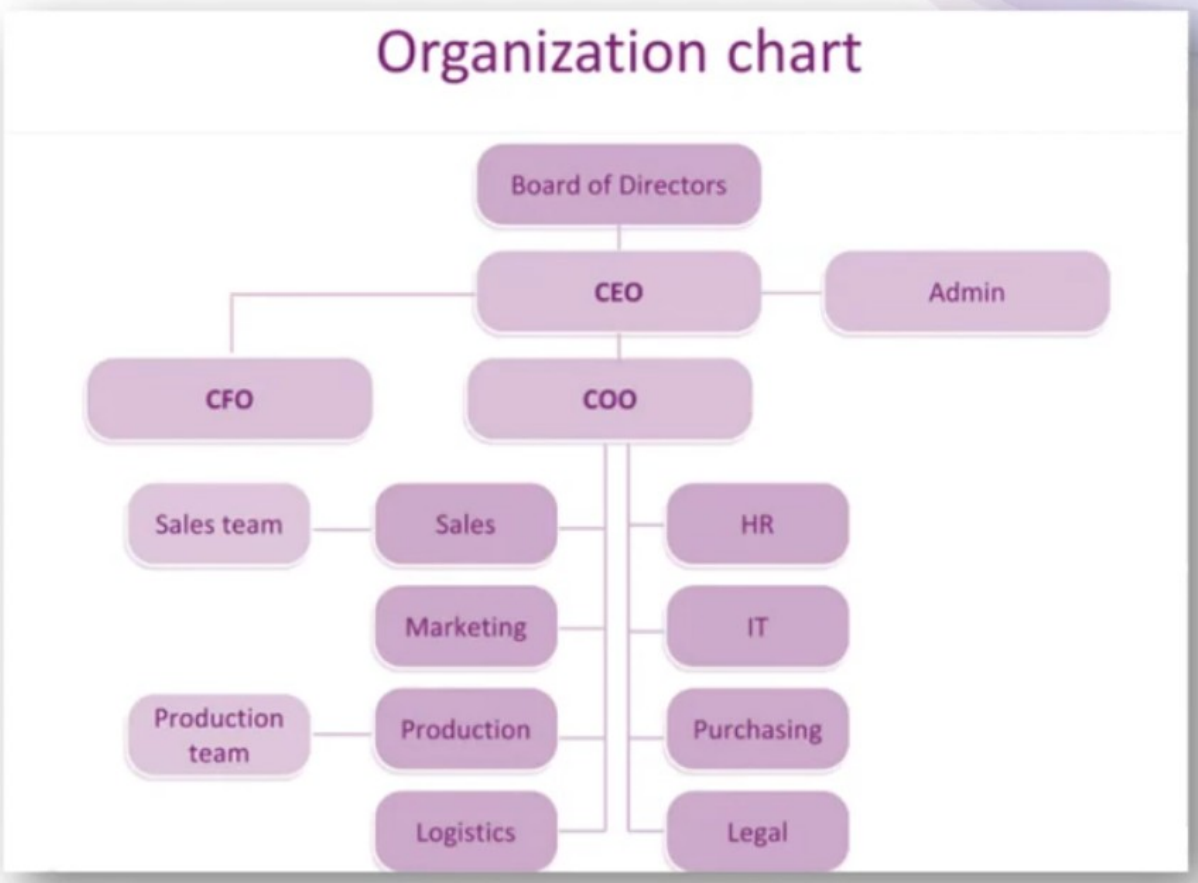
1. Implementing ISO 27001 is become official in the organization
2. Give authority to the project manager to enable him/her to succeed

Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

4.3 Determining the scope of the information security management system

You can implement the ISO 27001 Project on : process or processes, department(s), branch(es)

Ensure clear Scope in the ISMS Scope document (**department**, product, service, physical location, information systems)

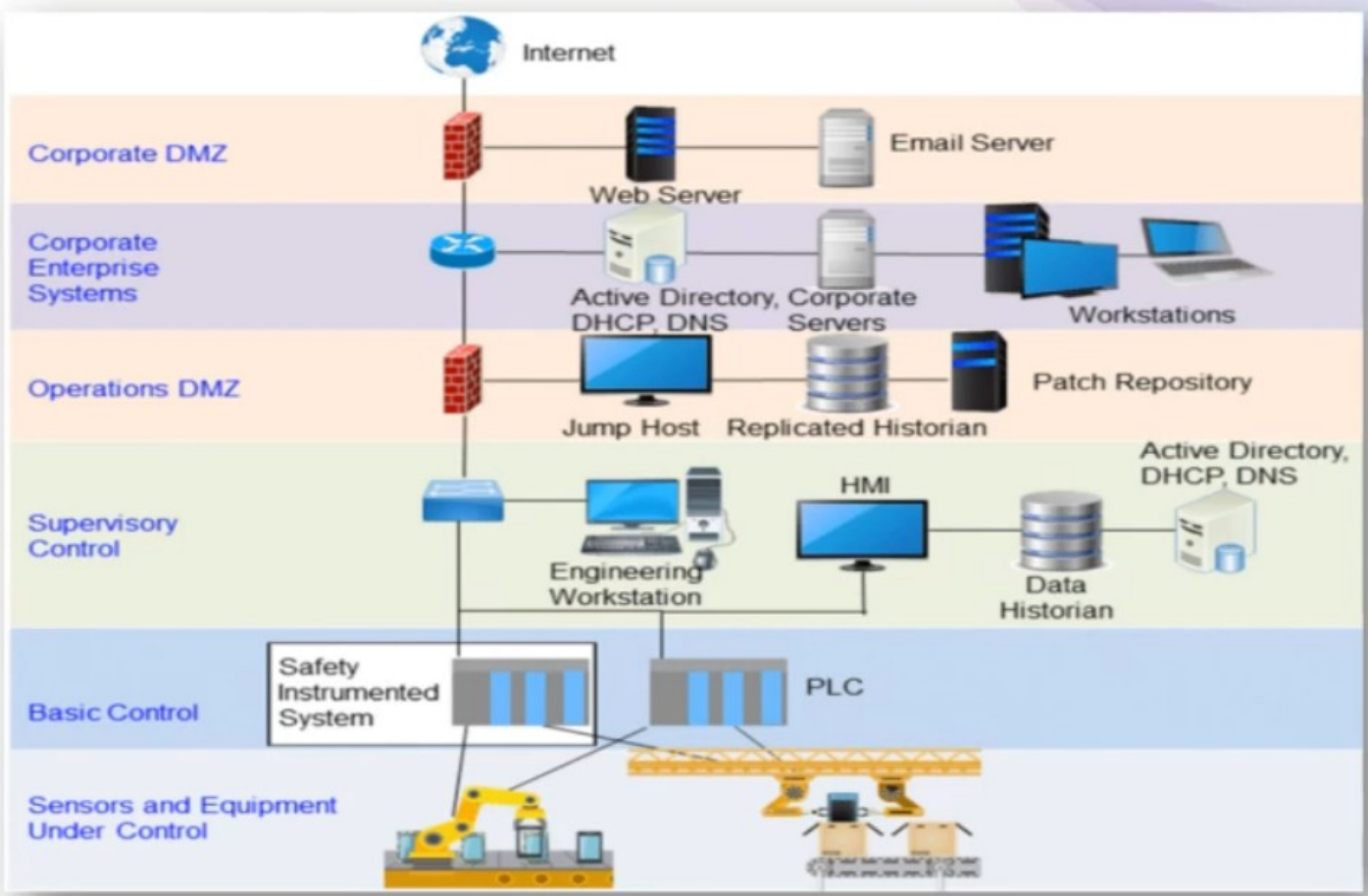


Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

4.3 Determining the scope of the information security management system

Ensure clear Scope in the ISMS Scope document (department, product, service, physical location, **information systems**)

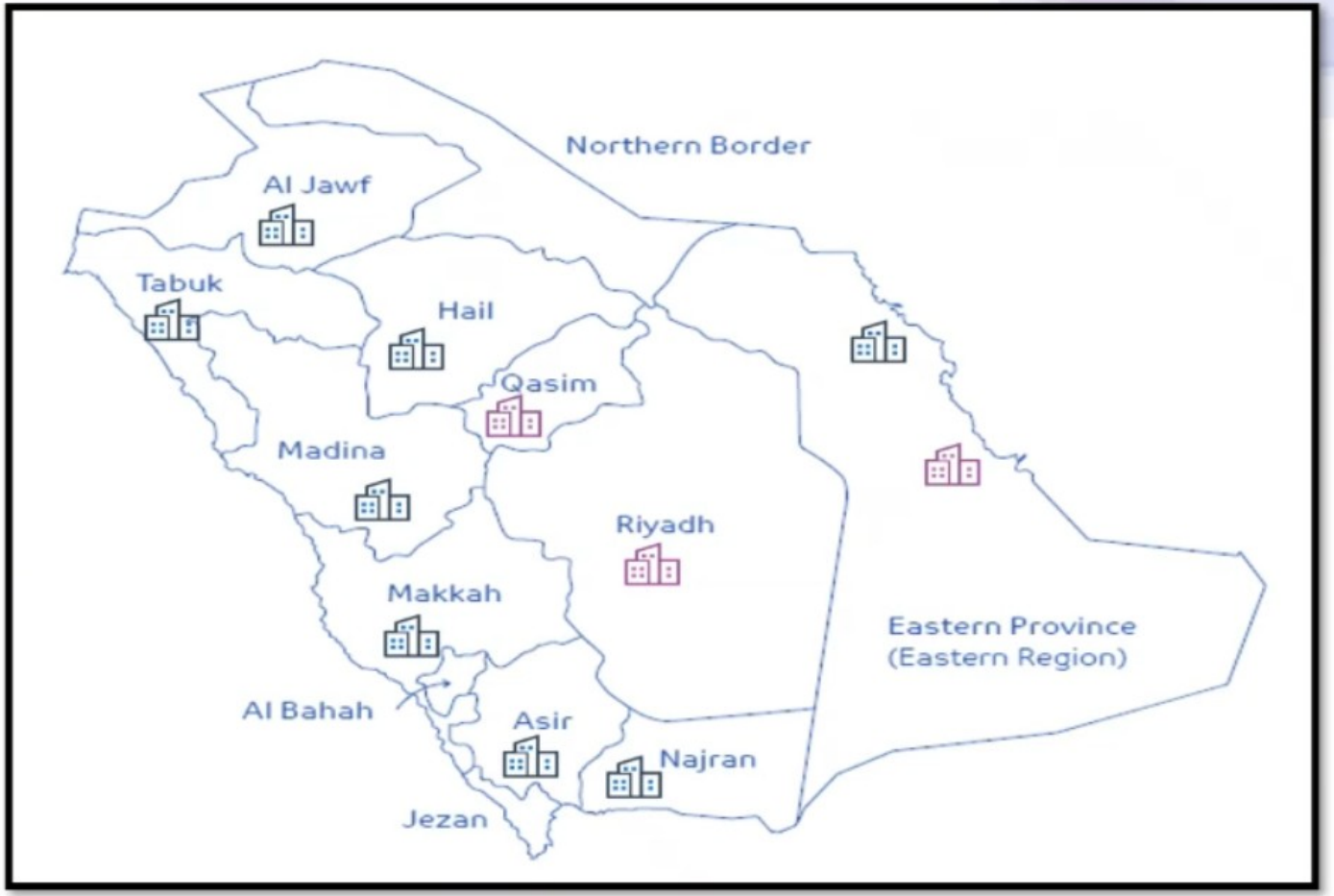
The boundaries of information systems is can be:
-Networks: internal networks, wireless networks, etc. ..
- OS: Windows, Linux, etc. ..
- Apps: CRM, software management payroll, ERP, utilities, database.
- Data: customer records, medical data, research and development, etc.
- Processes: Consider processes that transport, store or process information.
- Telecommunications equipment: routers, firewalls, etc.



Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

4.3 Determining the scope of the information security management system

Ensure clear Scope in the ISMS Scope document (department, product, service, **physical location**, information systems)



4 - Context of the Organization - Continued

Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

Example

The scope can be changed, minimized, extended and then it must be approved and documented

Bureau Veritas Certification

AEON THANA SINSAP (THAILAND) PUBLIC COMPANY LIMITED

Bureau Veritas Certification Holding SAS - UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013

Scope of certification

The following site is part of the Management System of the above organization

HEAD OFFICE

388 EXCHANGE TOWER, 26TH - 27TH &33RD - 34TH FLOOR, SUKHUMVIT ROAD, KHWAENG KLONGTOEY, KHET KLONGTOEY, BANGKOK 10110 THAILAND

RETAIL FINANCE BUSINESS COMPRISING CREDIT CARD, LOAN, HIRE PURCHASE MOTORCYCLE, WEB BUSINESS SERVICE AND USED CAR HIRE PURCHASE COVERING THE FOLLOWING DEPARTMENTS: FINANCE & ACCOUNTING SHARED SERVICE CENTER, SYSTEM PLANNING, I.T., SYSTEM DEVELOPMENT, MARKETING, CORPORATE GOVERNANCE & CONTROL, BUSINESS CONTROL MANAGEMENT AND LEGAL

STATEMENT OF APPLICABILITY (SOA), VERSION 2.0, EFFECTIVE DATE: NOVEMBER 03, 2014

Certificate No.: **TH015313-001** Version: 01 Issue Date: **18-06-2020**

The validity of this certificate depends on the validity of the main certificate

Certification Body Address: 5th Floor , 66 Prescot Street, London, E1 8HG, United Kingdom

Local office: Bureau Veritas Certification (Thailand) Ltd. 16th Floor, Bangkok Tower, 2170 New Petchburi Road, Bangkapi, Huaykwang, Bangkok 10310, Thailand

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.

To check this certificate validity please call: +662 670 4800

Context of the Organization - ISO/IEC 27001, clauses 4.3 and 4.4

4.4 Information security management system

The organization shall establish, implement, maintain and continually improve an information security management system, in accordance with the requirements of this International Standard.

How to achieve this control ?

Prepare a business case to convince the management and take their commitment on the ISO 27001 Implementation

Formalize a team to include

- **Project Sponsor:** provide the appropriate support and resources
  (Could be a committee)

- **Project Manager:** Define a project plan, monitor, manage the project on day to day
  (Should know skills in Project Management, have knowledge of information security, effective communication skills, analytical skills, leadership)

- **Project Team:** Implement the ISO 27001 Standard

4 - Context of the Organization - overall

5 - Leadership and Management Commitment

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment with respect to the information security management system by:

- A .ensuring the information security policy and the information security objectives are established and are compatible with the strategic direction of the organization
- B. ensuring the integration of the information security management system requirements into the organization's processes
- C. ensuring that the resources needed for the information security management system are available
- D. communicating the importance of effective information security management and of conforming to the information security management system requirements
- E. ensuring that the information security management system achieves its intended outcome(s);
- F. directing and supporting persons to contribute to the effectiveness of the information security management system
- G. promoting continual improvement
- H. supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

5 - Leadership and Management Commitment - Continued

ISO/IEC 27001, clause 5.2 - Policy

Top management shall establish an information security policy that:

A. is appropriate to the purpose of the organization
B. provides a framework for setting information security objectives
C. includes a commitment to satisfy applicable requirements
D. includes a commitment to continual improvement of the ISMS

The information security policy shall:

E. be available as documented information
F. be communicated within the organization
G. be available to interested parties, as appropriate.

ISO/IEC 27001, clause 5.2 - Policy

Top management shall establish an information security policy that:

A. is appropriate to the purpose of the organization
B. provides a framework for setting information security objectives
C. includes a commitment to satisfy applicable requirements
D. includes a commitment to continual improvement of the ISMS

The information security policy shall:

E. be available as documented information
F. be communicated within the organization
G. be available to interested parties, as appropriate.


ABC Company

Cyber Security Policy

XXX -PL###

Version X.X

19 June 2021

© 2021 ABC

All rights reserved. All information contained in this document is confidential and proprietary to ABC. No part of this document may be photocopied, electronically transferred, modified, or reproduced in any manner without the prior written consent of ABC.

Quick Tips when start developing Policies

1- Create a policy that reflect the organization's business situation, culture, issues and concerns relating to information security.
2- Be simple in choosing the concepts (pretend to be a normal user - not cybersecurity officer)
3- High level statements
4- Answer the “WHY” Question.

ISO/IEC 27001, clause 5.2 - Policy

Top management shall establish an information security policy that:

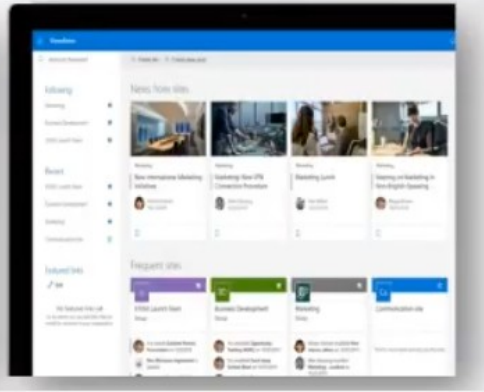
A. is appropriate to the purpose of the organization
B. provides a framework for setting information security objectives
C. includes a commitment to satisfy applicable requirements
D. includes a commitment to continual improvement of the ISMS

The information security policy shall:

E. be available as documented information
F. be communicated within the organization
G. be available to interested parties, as appropriate.

Communicate the policy through

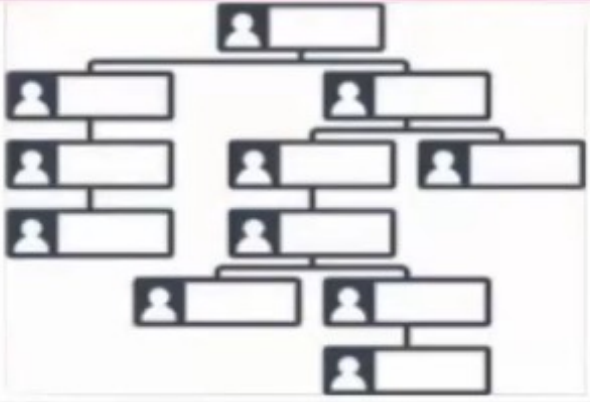
1- Print it and publish on the company premise
2- SharePoint
3- Email
4- Orientation and Awareness sessions



5 - Organizational roles, responsibilities & authorities

ISO/IEC 27001, clause 5.3

- Top management shall ensure that the responsibilities and authorities for relevant roles are assigned and communicated within the organization
- Top management shall assign the responsibility and authority for:
  A. Ensuring that the information security management system is established and implemented in accordance with the requirements of ISO/IEC 27001
  B. Reporting on the performance of the ISMS to top management



6 - Planning

6.1 Actions to address risks and opportunities

Def# - Vulnerability, Threat and Impact

Vulnerability means weakness of an asset or control that can be exploited by one or more threats. (Could be intrinsic or extrinsic)

Examples of vulnerability:
1- Unpatched Systems or software
2- Undefined proper roles and responsibilities in information security
3- No awareness of staff related to information security
4- Lack of software testing
5- Lack of backup process

Def# - Vulnerability, Threat and Impact

Threat means a potential cause of an unwanted incident, which can result in harm to a system or organization

Examples of threats:
1- Natural events (flood, earthquake, volcano, etc.)
2- Loss of power supply
3- Data Theft
4- Data Corruption
5- Server Failure / Crash

6 – Planning - Continued

6.1 Actions to address risks and opportunities

Def# - Vulnerability, Threat and Impact

Impact means what is the effect after the occurrence of breaching C,I,A

Examples of impact on confidentiality:
1- Confidential information leakage
2- Invasion of privacy of employees
3- Lawsuits and penalties

Examples of impact on Integrity:
1- Incorrect results
2- Manipulated Data

Examples of impact on Availability:
1- System/ Service Unavailable
2- Operation Disruptions
3- Financial loss

6 – Planning - Continued

6.1 Actions to address risks and opportunities

Definition of Information Security Risk as per ISO/IEC 27000, clause 3.61

- Information security risk is associated with the potential that threats will exploit vulnerabilities of an information asset or group of information assets and thereby cause harm to an organization.
- Risk is often expressed in terms of a combination of the consequences of an event (including changes in circumstances) and the associated "likelihood" of occurrence.
- As per ISO 27005 Standard, Risk Formula is Impact X Likelihood

- Residual Risk: Risk remaining after risk treatment.
- Risk Acceptance: Informed decision to take a particular risk.
- Risk Analysis: Process to comprehend the nature of risk and to determine the level of risk.
- Risk Assessment: Overall process of risk identification, risk analysis and risk evaluation.
- Risk Evaluation: Process of comparing the results of risk analysis with risk criteria to determine whether the risk and/or its magnitude is acceptable or tolerable.
- Risk Management: Coordinated activities to direct and control an organization with regard to risk.
- Risk Treatment: Process to modify risk.

6 – Planning - Continued

6.1 Actions to address risks and opportunities

6.1.1 General

- When planning for the information security management system, the organization shall consider the issues referred in 4.1 (Understanding the organization and its context) and the requirements referred to in 4.2 (Understanding the needs and expectations of interested parties) and determine the risks and opportunities that need to be addressed to:
  a) Ensure the information security management system can achieve its intended outcome(s)
  b) Prevent, or reduce, undesired effects; and
  c) Achieve continual improvements,

  The Organization shall plan:

  d) Actions to address these risks and opportunities; and
  e) How to:

     1) integrate and implement the actions into its information security management system processes; and
     2) evaluate the effectiveness of these actions.

6 – Planning - Continued

6.1 Actions to address risks and opportunities

6.1.2 Information security risk assessment

- The organization shall define and apply an information security risk assessment process that:
  a) Establishes and maintains information security risk criteria that include:
  1. The risk acceptance criteria; and
  2. Criteria for performing information security risk assessments;

  b) Ensures that repeated information security risk assessments produce consistent, valid and comparable results;

  c) Identifies the information security risks
  1. apply the information security risk assessment process to identify risks associated with the loss of confidentiality, integrity and availability for information within the scope of the information security management system; and
  2. identify the risk owners;

6 – Planning - Continued

6.1 Actions to address risks and opportunities

6.1.2 Information security risk assessment

- The organization shall define and apply an information security risk assessment process that:
  d) analyses the information security risks:
    1) assess the potential consequences that would result if the risks identified in 6.1.2 c) 1) were to materialize;
    2) assess the realistic likelihood of the occurrence of the risks identified in 6.1.2. c) 1); and
    3) determine the levels of risk;

  e) evaluates the information security risks:
    1) compare the results of risk analysis with the risk criteria established in 6.1.2. a); and
    2) prioritize the analysed risks for risk treatment.

  The organization shall retain documented information about the information security risk assessment process.

6 – Planning - Continued

6.1 Actions to address risks and opportunities

6.1.3 Information security risk treatment

- The organization shall define and apply an information security risk treatment process to:

  a) select appropriate information security risk treatment options, taking account of the risk assessment results;
  b) determine all controls that are necessary to implement the information security risk treatment option(s) chosen

NOTE Organizations can design controls as required, or identify them from any source.

  c) compare the controls determined in 6.1.3 b) above with those in Annex A and verify that no necessary controls have been omitted;
  d) produce a Statement of Applicability that contains the necessary controls (see 6.1.3. b) and c)) and justification for inclusions, whether they are implemented or not, and the justification for exclusions of controls from Annex A;
  e) formulate an information security risk treatment plan; and
  f) obtain risk owners' approval of the information security risk treatment plan and acceptance of the residual information security risks.

The organization shall retain documented information about the information security risk treatment process.

6 – Planning - Continued

6.2 Information security objectives and planning to achieve them

- The organization shall establish information security objectives at relevant functions and levels. The information security objectives shall:
  - a) be consistent with the information security policy;
  - b) be measurable (if practicable);
  - c) take into account applicable information security requirements, and results from risk assessment and risk treatment;
  - d) be communicated; and
  - e) be updated as appropriate.

The organization shall retain documented information on the information security objectives. When planning how to achieve its information security objectives, the organization shall determine:

- f) what will be done;
- g) what resources will be required;
- h) who will be responsible;
- i) when it will be completed; and
- j) how the results will be evaluated.

Overview of Risk Management

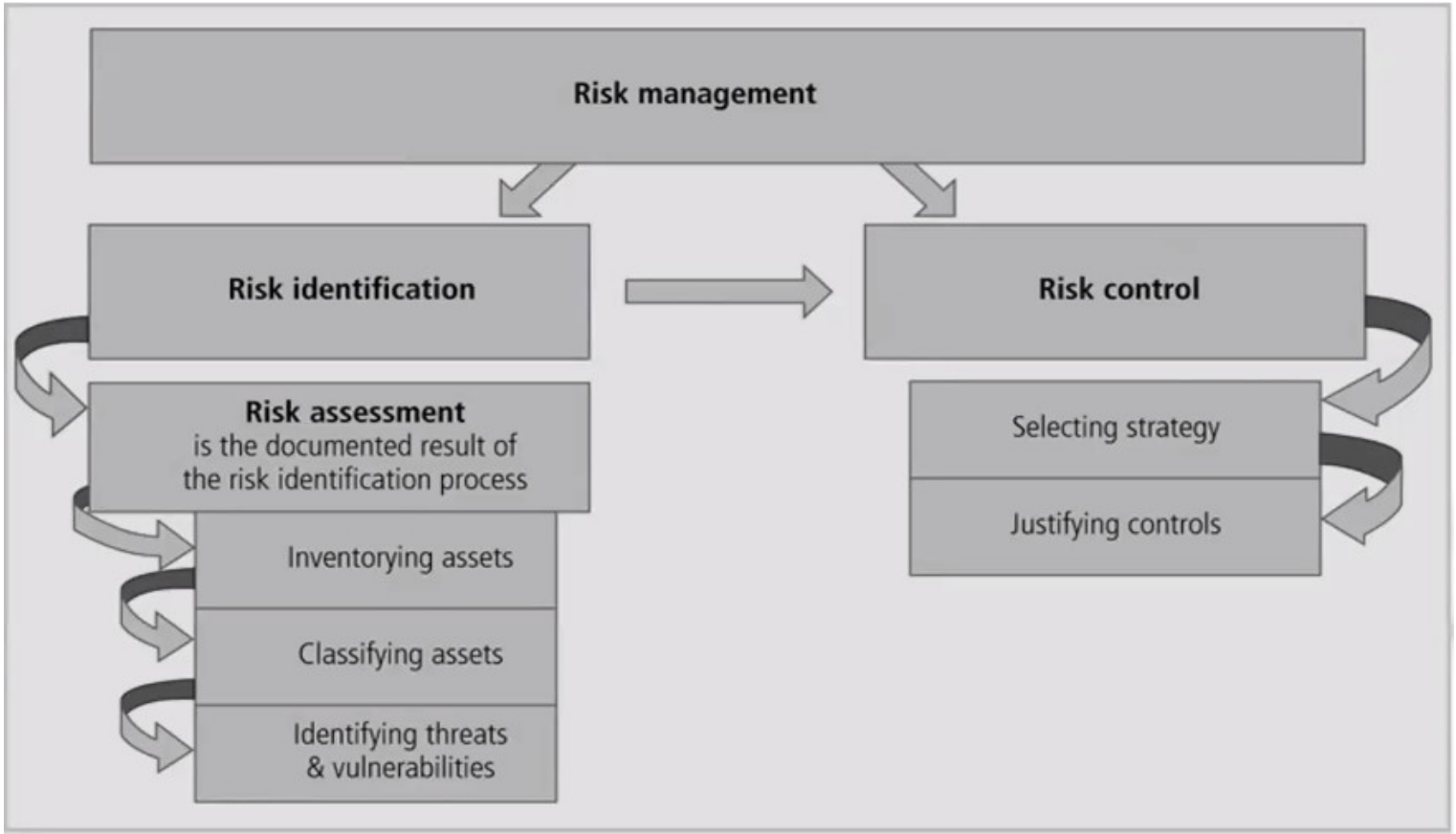


FIGURE 1-2 Components of risk management

II.1. Risk Identification

Identify, classify, and prioritize information assets

Goal: protect assets from threats

Identify threats

Identify vulnerabilities of each asset

Identify controls that will limit possible losses in the event of attack

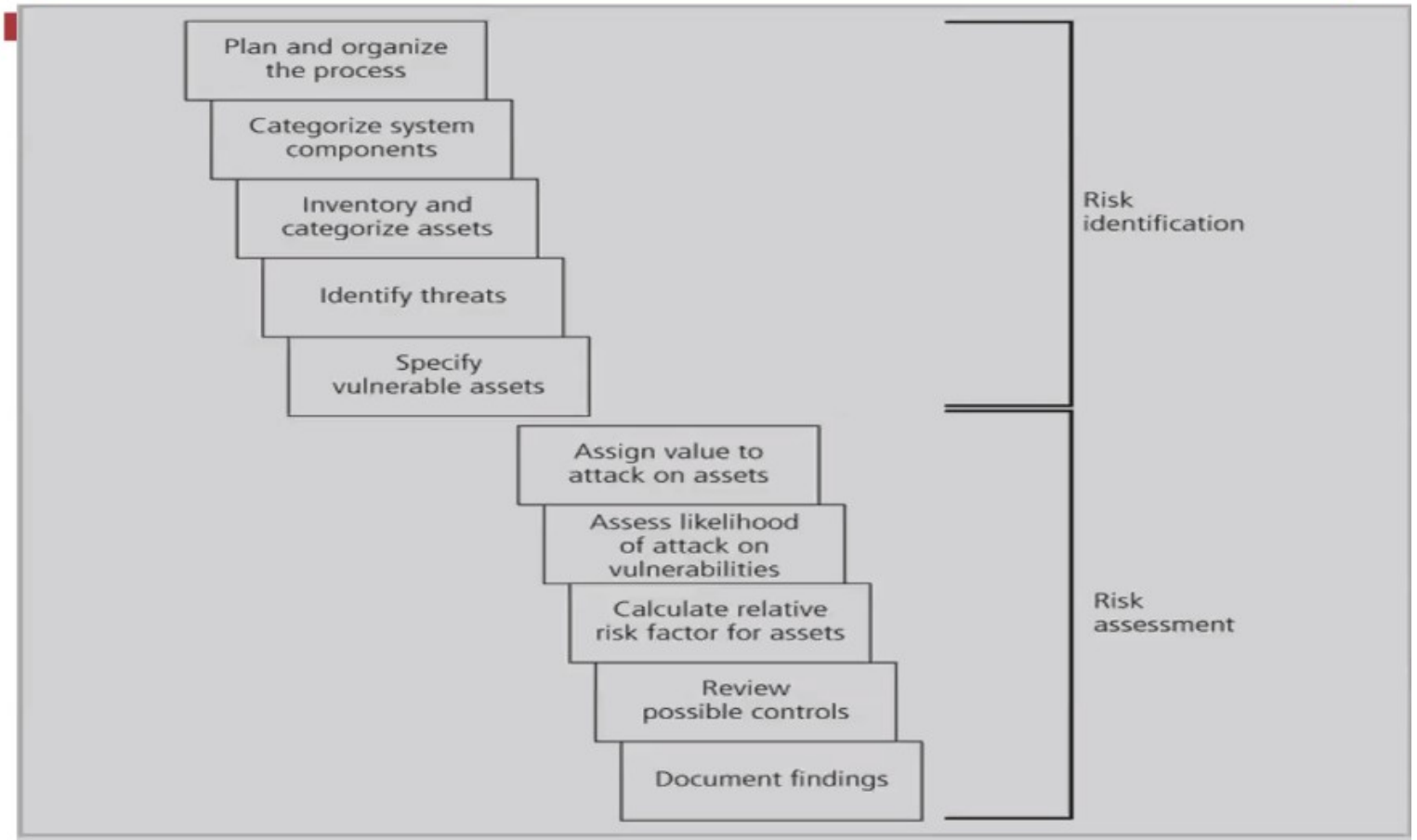


FIGURE 1-3 Components of risk identification

II. 1 Risk Assessment

Risk assessment:

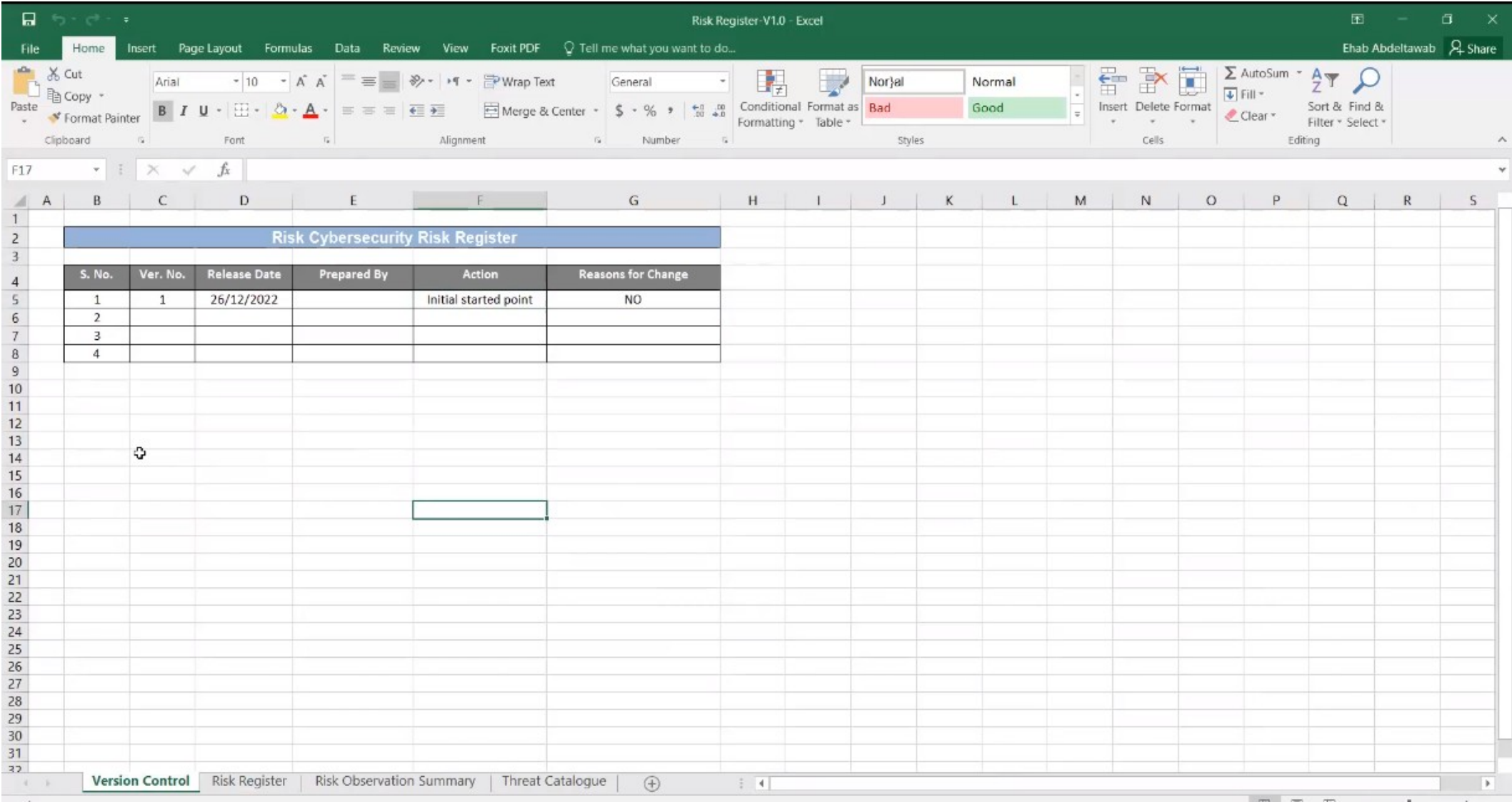
- Process of assigning a risk rating or score to each information asset
- Goal is to determine the relative risk of each vulnerability using various factors

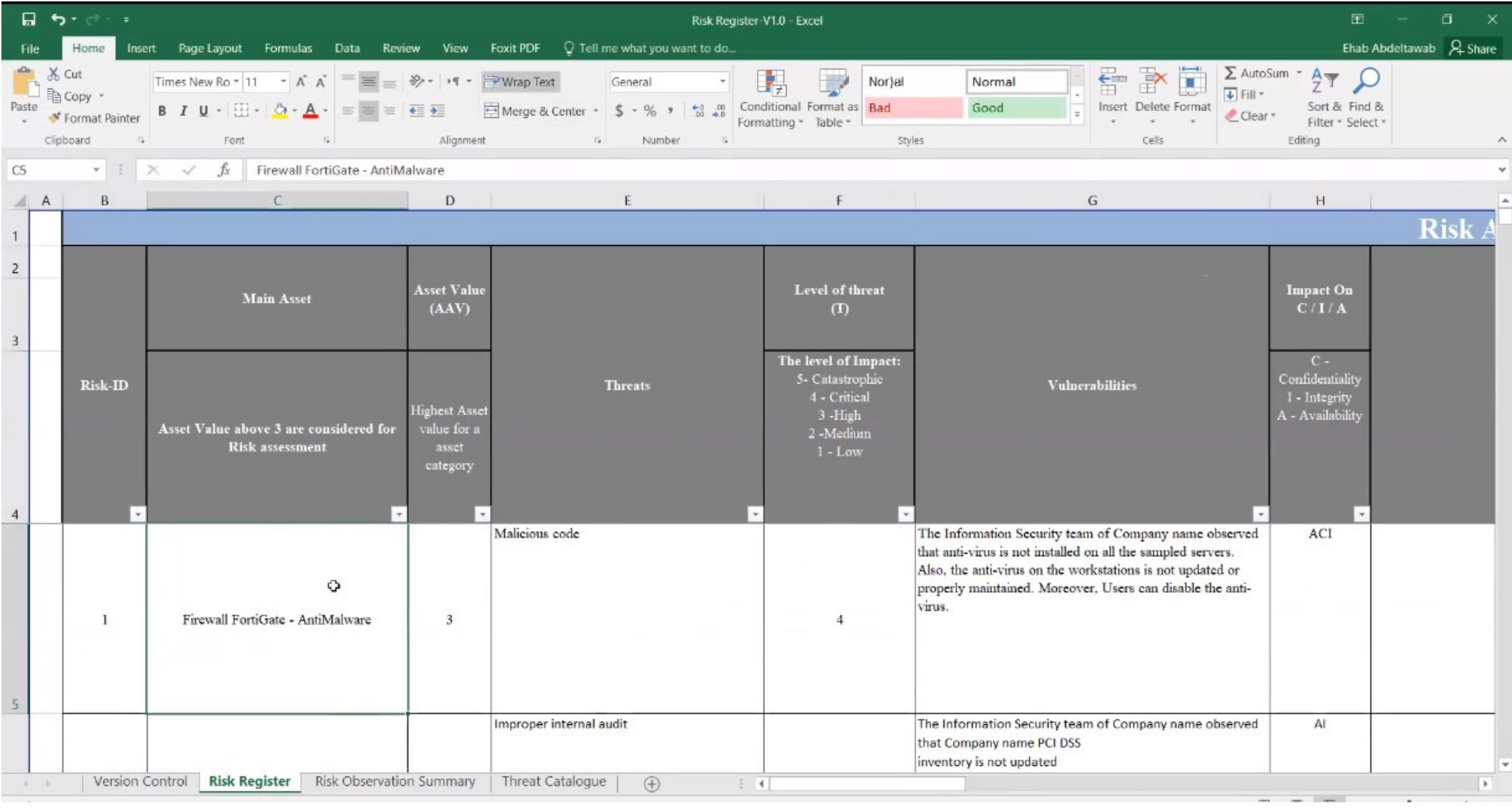
Likelihood:

- Probability that a specific vulnerability will be successfully attacked
- Many asset/vulnerability combinations have external references for likelihood values

Example of a weighted factor analysis worksheet

Information Asset	Criteria 1: Impact to Revenue	Criteria 2: Impact to Profitability	Criteria 3: Public Image Impact	Weighted Score
Criterion Weight (1–100) Must total 100	30	40	30	
EDI Document Set 1—Logistics BOL to outsourcer (outbound)	0.8	0.9	0.5	75
EDI Document Set 2—Supplier orders (outbound)	0.8	0.9	0.6	78
EDI Document Set 2—Supplier fulfillment advice (inbound)	0.4	0.5	0.3	41
Customer order via SSL (inbound)	1.0	1.0	1.0	100
Customer service request via e-mail (inbound)	0.4	0.4	0.9	55


Risk Register-V1.0 - Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Foxit PDF
Tell me what you want to do...
Ehab Abdeltawab
Share
Cut
Copy
Format Painter
Paste
Arial
10
Wrap Text
Merge & Center
General
Conditional Formatting
Format as Table
Normal
Bad
Good
Insert
Delete
Format
AutoSum
Fill
Clear
Sort & Filter
Find & Select
Clipboard
Font
Alignment
Number
Styles
Cells
Editing
F17
Risk Cybersecurity Risk Register
S. No.
Ver. No.
Release Date
Prepared By
Action
Reasons for Change
1
1
26/12/2022
Initial started point
NO
2
3
4
Version Control
Risk Register
Risk Observation Summary
Threat Catalogue


Risk Register-V1.0 - Excel
File
Home
Insert
Page Layout
Formulas
Data
Review
View
Foxit PDF
Tell me what you want to do...
Ehab Abdeltawab
Share
Cut
Copy
Format Painter
Paste
Times New Ro
11
Wrap Text
Merge & Center
General
Conditional Formatting
Format as Table
Normal
Bad
Good
Insert
Delete
Format
AutoSum
Fill
Clear
Sort & Filter
Find & Select
Clipboard
Font
Alignment
Number
Styles
Cells
Editing
C5
Firewall FortiGate - AntiMalware
Risk-ID
Main Asset
Asset Value above 3 are considered for Risk assessment
Asset Value (AAV)
Highest Asset value for a asset category
Threats
Level of threat (T)
The level of Impact:
5- Catastrophic
4 - Critical
3 -High
2 -Medium
1 - Low
Vulnerabilities
Impact On C / I / A
C - Confidentiality
I - Integrity
A - Availability
1
Firewall FortiGate - AntiMalware
3
Malicious code
4
The Information Security team of Company name observed that anti-virus is not installed on all the sampled servers. Also, the anti-virus on the workstations is not updated or properly maintained. Moreover, Users can disable the anti-virus.
ACI
Improper internal audit
The Information Security team of Company name observed that Company name PCI DSS inventory is not updated
AI
Version Control
Risk Register
Risk Observation Summary
Threat Catalogue

THANKS!