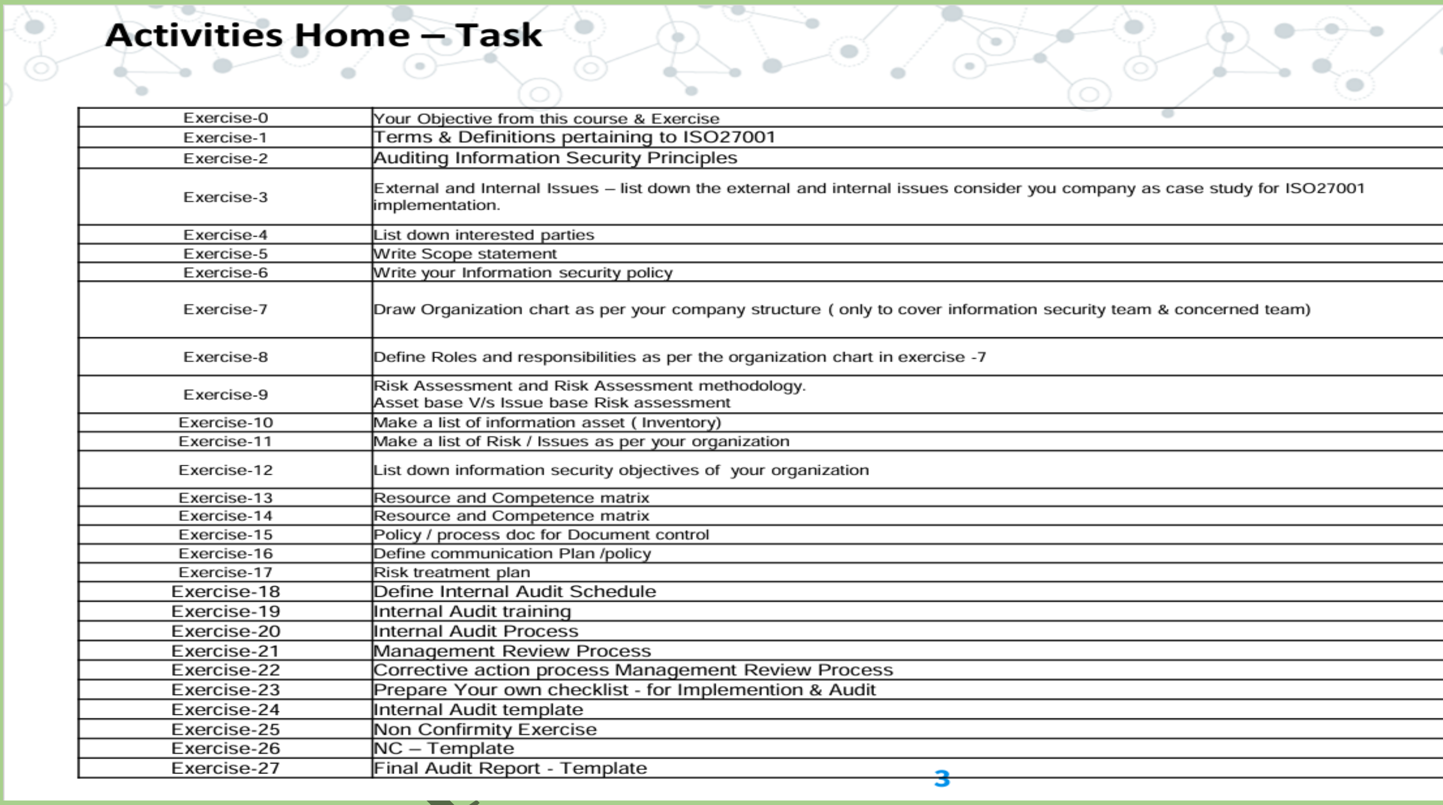
ISO / IEC 27001:2022 Lead Implementer Course – Expert Guide

ISO 27001 Lead Implementer Certification does not only apply to information security. All the policies and controls under this standard are given to the whole organization. Hence, they can serve all the department



Activities Home – Task

Exercise-0	Your Objective from this course & Exercise
Exercise-1	Terms & Definitions pertaining to ISO27001
Exercise-2	Auditing Information Security Principles
Exercise-3	External and Internal Issues – list down the external and internal issues consider you company as case study for ISO27001 implementation.
Exercise-4	List down interested parties
Exercise-5	Write Scope statement
Exercise-6	Write your Information security policy
Exercise-7	Draw Organization chart as per your company structure (only to cover information security team & concerned team)
Exercise-8	Define Roles and responsibilities as per the organization chart in exercise -7
Exercise-9	Risk Assessment and Risk Assessment methodology. Asset base V/s Issue base Risk assessment
Exercise-10	Make a list of information asset (Inventory)
Exercise-11	Make a list of Risk / Issues as per your organization
Exercise-12	List down information security objectives of your organization
Exercise-13	Resource and Competence matrix
Exercise-14	Resource and Competence matrix
Exercise-15	Policy / process doc for Document control
Exercise-16	Define communication Plan /policy
Exercise-17	Risk treatment plan
Exercise-18	Define Internal Audit Schedule
Exercise-19	Internal Audit training
Exercise-20	Internal Audit Process
Exercise-21	Management Review Process
Exercise-22	Corrective action process Management Review Process
Exercise-23	Prepare Your own checklist - for Implemention & Audit
Exercise-24	Internal Audit template
Exercise-25	Non Confirmity Exercise
Exercise-26	NC – Template
Exercise-27	Final Audit Report - Template

3

Clause 5: Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibility and authorities

5.1 Leadership and Commitment

Top management shall determine and demonstrate commitment by:

- Ensuring information security policy and security objectives are met
- Ensuring resources needed for the information security management system are available
- Communicating the importance of effective information security management
- Promoting continual improvement

5.2 Policy

The management shall establish an information security that:

- Is appropriate to the purpose of the organization
- Includes information security objectives
- It satisfies applicable requirements related to information security
- Display a commitment to continual improvement

The information security policy shall:

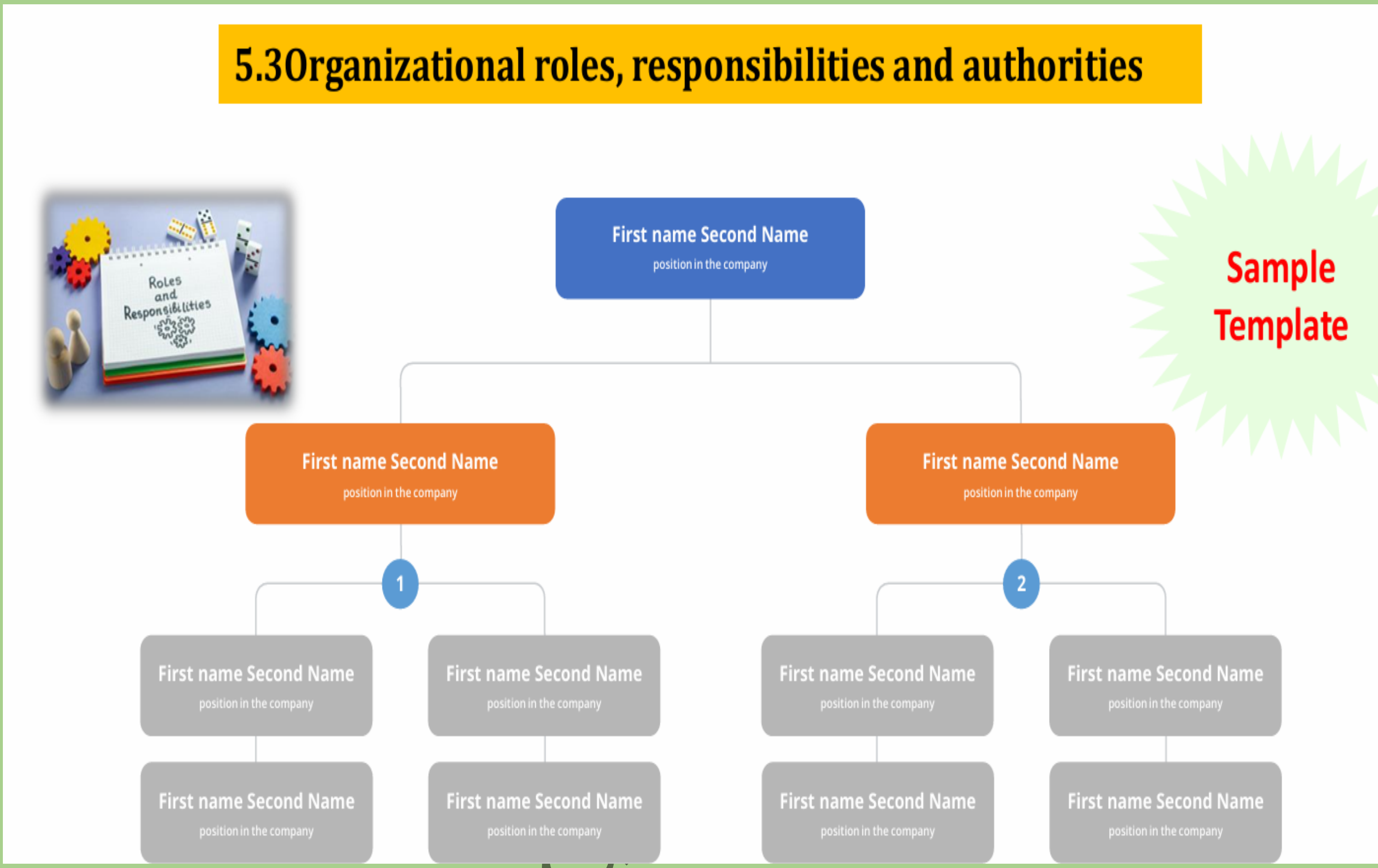
- Be available as documented information
- Be communicated within the organization
- Be available to interested parties, as appropriate

Exercise 9:

- Write your own information security policy
- Considering your company as a case study for ISO 27001:2022 implementation
- Template sample: https://www.linkedin.com/pulse/example-information-security-policy-iso27001-clause-52-chris-hall/

5.3 Organizational roles, responsibilities and authorities

- If you are given some responsibilities then you need to have authority for you to perform roles effectively
- Roles should be well defined and communicated within the organization
- It is the responsibility of the top management to assign roles to ensure that information security within the organization meets the standard
- If you have been assigned some tasks by the top management, then it is your responsibility to write a report from the activity
- Below is a sample of an Organization Security policy. Note that you should stick to the aspect of information security policy



5.3Organizational roles, responsibilities and authorities

Exercise 10:

- Draw an organization chart as per your company structure only to cover information security team and concerned team) you can seek help from HR. Department for roles and responsibilities
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 11:

- Define roles and responsibilities as per the organizational chart in exercise - 10

Clause 6: Planning

6.1 Actions to address risks and opportunities

6.2 Information security risk assessment

6.3 Information security objectives and planning to achieve them

6.1 Actions to address risks and opportunities

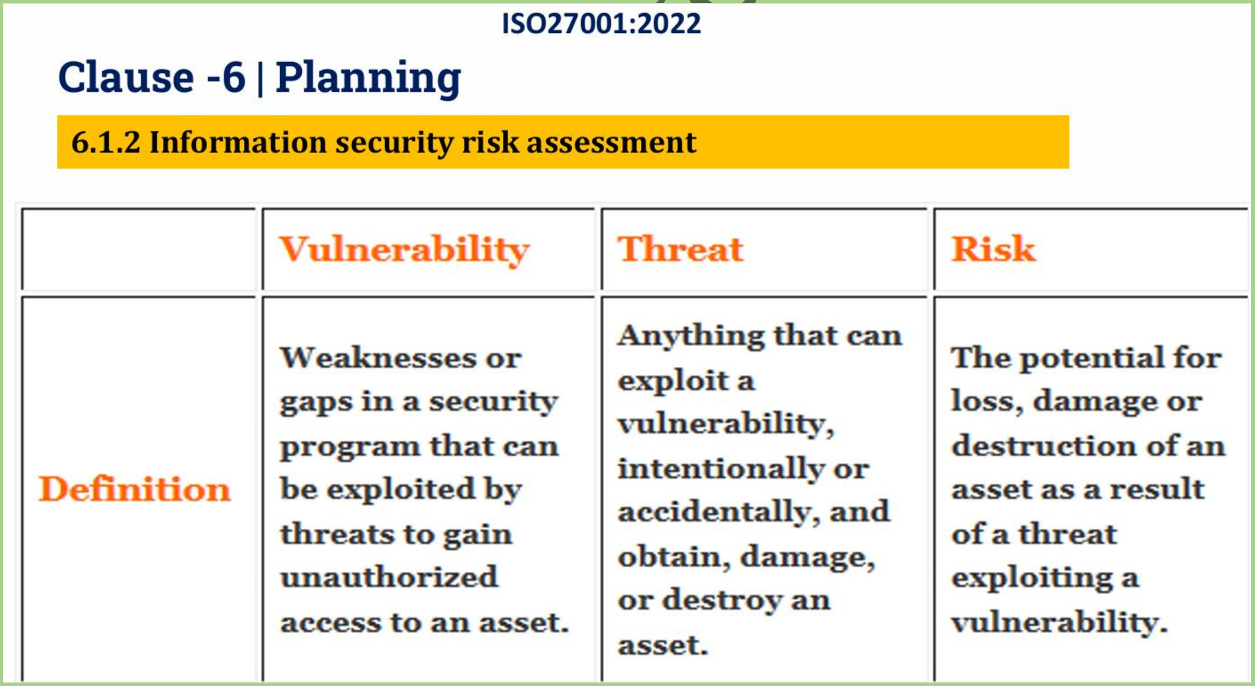
- When planning for information security management the organization shall consider the issued referred in Sub-CL 4.1 and requirements referred to in Sub-CL 4.2 and determine the risk opportunities that need to be addressed
- The organization shall plan on how to tackle the identified risk opportunities and lay out mitigation protocols

6.2 Information security risk assessment

The management shall establish and maintain information security criteria which includes:

- Risk assessment criteria
- Criteria for performing risk assessment criteria
- Identify risk owners
- Identify the likelihood of consequences if the risks were materialized
- Access the realistic likelihood of the occurrence of the risks identified
- You are first going to identify the risks in Sub-CL 4.1 and Sub-CL 4.2

The 3 magical words in risk assessment:



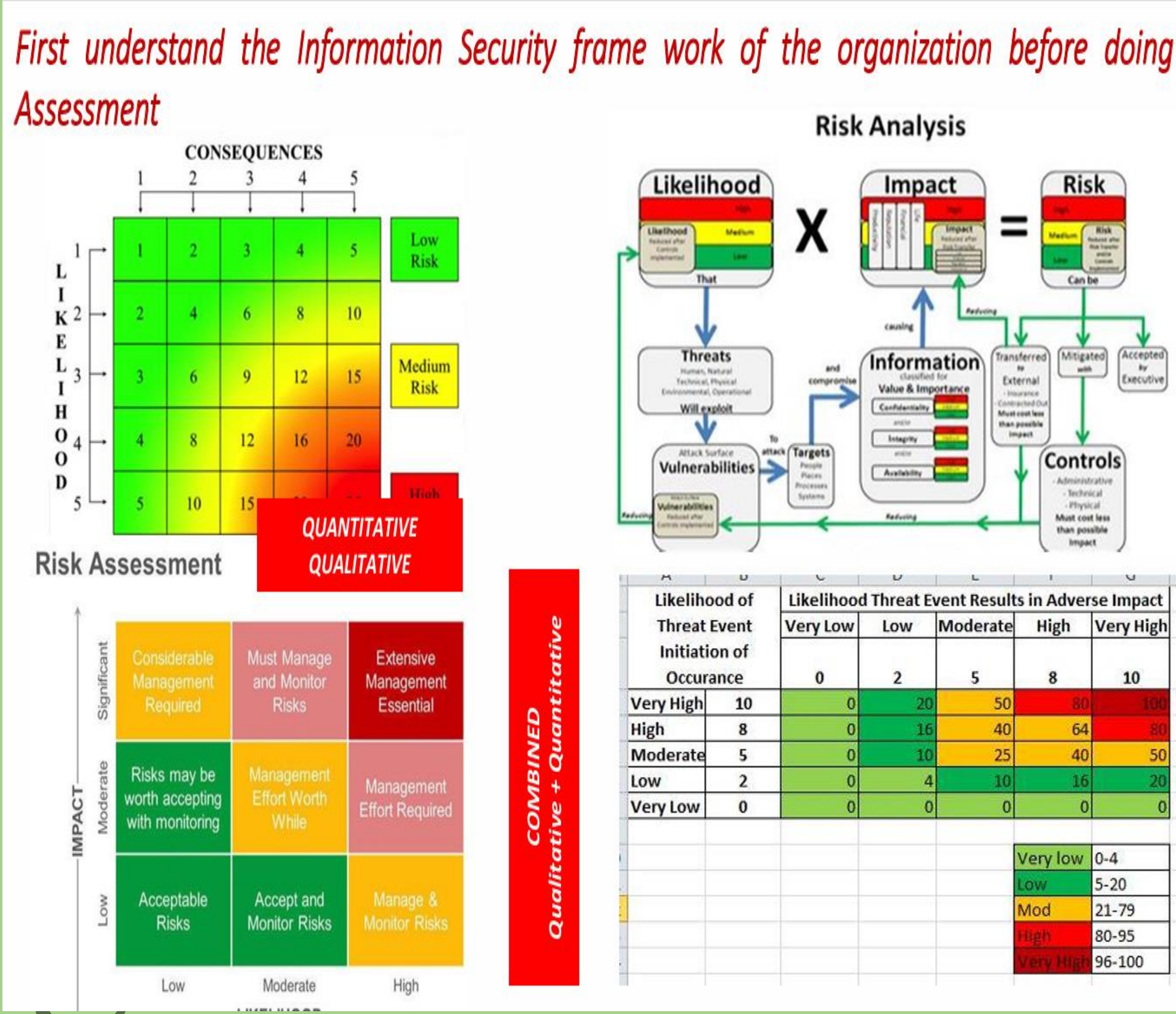
ISO27001:2022

Clause -6 | Planning

6.1.2 Information security risk assessment

	Vulnerability	Threat	Risk
Definition	Weaknesses or gaps in a security program that can be exploited by threats to gain unauthorized access to an asset.	Anything that can exploit a vulnerability, intentionally or accidentally, and obtain, damage, or destroy an asset.	The potential for loss, damage or destruction of an asset as a result of a threat exploiting a vulnerability.

Before doing the risk assessment first, you need to understand the framework of the organization first



First understand the Information Security frame work of the organization before doing Assessment

CONSEQUENCES

	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15		

LIKELIHOOD

Low Risk

Medium Risk

High

QUANTITATIVE
QUALITATIVE

Risk Assessment

IMPACT			
Significant	Considerable Management Required	Must Manage and Monitor Risks	Extensive Management Essential
Moderate	Risks may be worth accepting with monitoring	Management Effort Worth While	Management Effort Required
Low	Acceptable Risks	Accept and Monitor Risks	Manage & Monitor Risks
	Low	Moderate	High

COMBINED
Qualitative + Quantitative

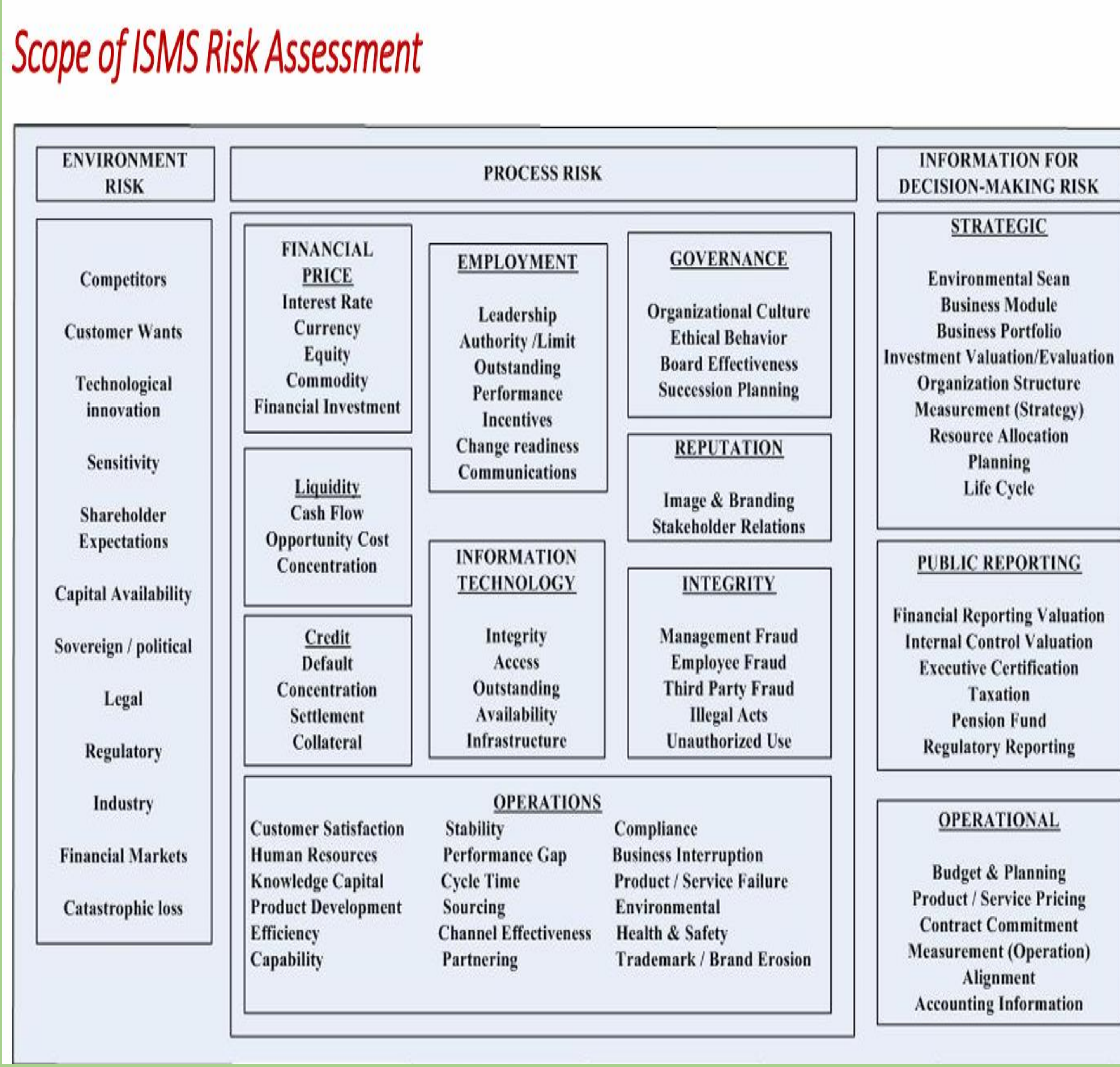
Risk Analysis

Likelihood of Threat Event Initiation of Occurance		Likelihood Threat Event Results in Adverse Impact				
		Very Low	Low	Moderate	High	Very High
		0	2	5	8	10
Very High	10	0	20	50	80	100
High	8	0	16	40	64	80
Moderate	5	0	10	25	40	50
Low	2	0	4	10	16	20
Very Low	0	0	0	0	0	0

Very low	0-4
Low	5-20
Mod	21-79
High	80-95
Very High	96-100

Also, you need to understand the locations

You can categorize the risk assessment in the case of multiprocesses



Scope of ISMS Risk Assessment

ENVIRONMENT RISK

Competitors

Customer Wants

Technological innovation

Sensitivity

Shareholder Expectations

Capital Availability

Sovereign / political

Legal

Regulatory

Industry

Financial Markets

Catastrophic loss

PROCESS RISK

FINANCIAL

PRICE

Interest Rate
Currency
Equity
Commodity
Financial Investment

Liquidity

Cash Flow
Opportunity Cost
Concentration

Credit

Default
Concentration
Settlement
Collateral

EMPLOYMENT

Leadership
Authority /Limit
Outstanding
Performance
Incentives
Change readiness
Communications

INFORMATION TECHNOLOGY

Integrity
Access
Outstanding
Availability
Infrastructure

GOVERNANCE

Organizational Culture
Ethical Behavior
Board Effectiveness
Succession Planning

REPUTATION

Image & Branding
Stakeholder Relations

INTEGRITY

Management Fraud
Employee Fraud
Third Party Fraud
Illegal Acts
Unauthorized Use

OPERATIONS

Customer Satisfaction
Human Resources
Knowledge Capital
Product Development
Efficiency
Capability

Stability
Performance Gap
Cycle Time
Sourcing
Channel Effectiveness
Partnering

Compliance
Business Interruption
Product / Service Failure
Environmental
Health & Safety
Trademark / Brand Erosion

INFORMATION FOR DECISION-MAKING RISK

STRATEGIC

Environmental Sean
Business Module
Business Portfolio
Investment Valuation/Evaluation
Organization Structure
Measurement (Strategy)
Resource Allocation
Planning
Life Cycle

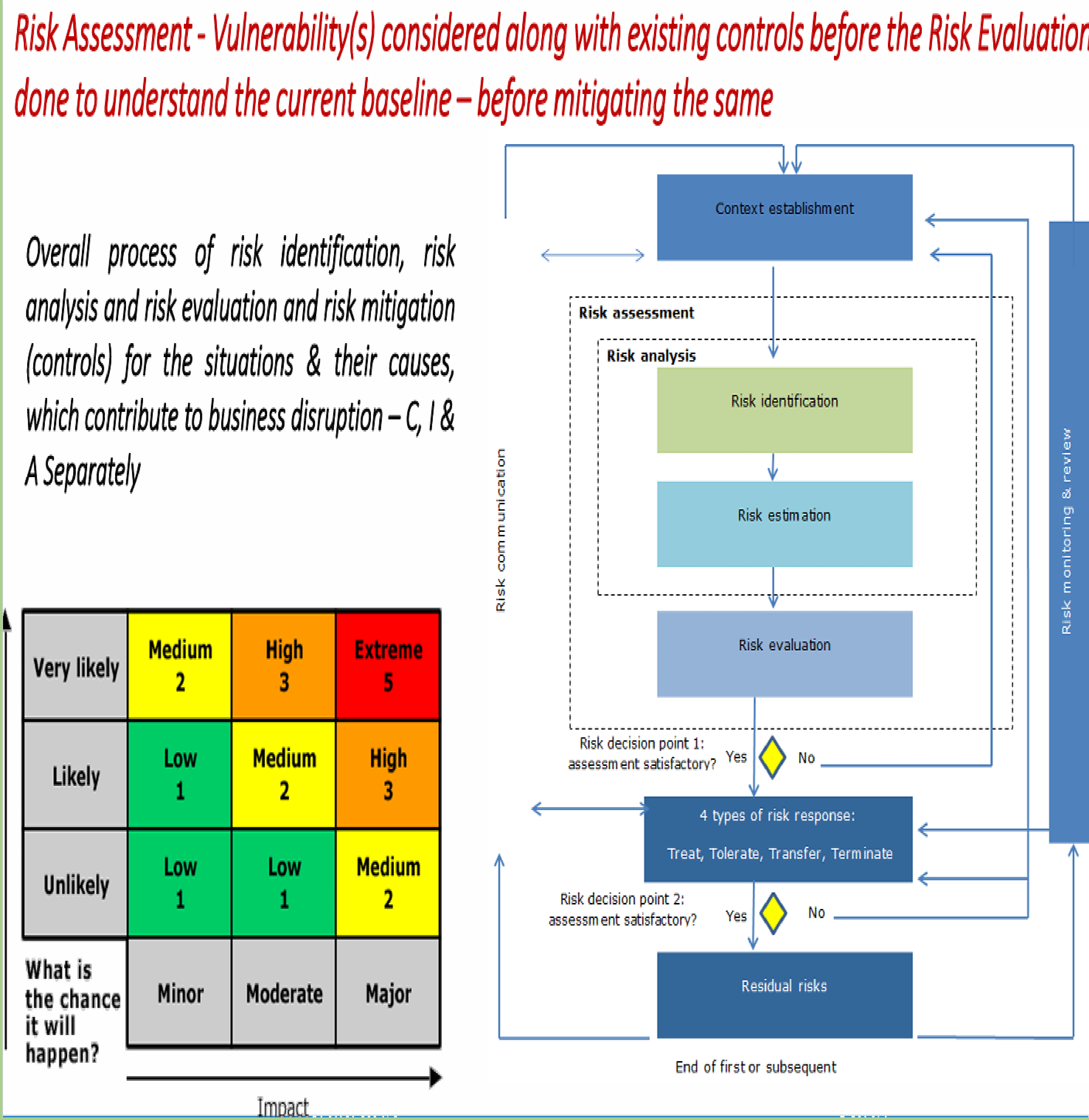
PUBLIC REPORTING

Financial Reporting Valuation
Internal Control Valuation
Executive Certification
Taxation
Pension Fund
Regulatory Reporting

OPERATIONAL

Budget & Planning
Product / Service Pricing
Contract Commitment
Measurement (Operation)
Alignment
Accounting Information

Below is the overall overview of risk identification, analysis and mitigation



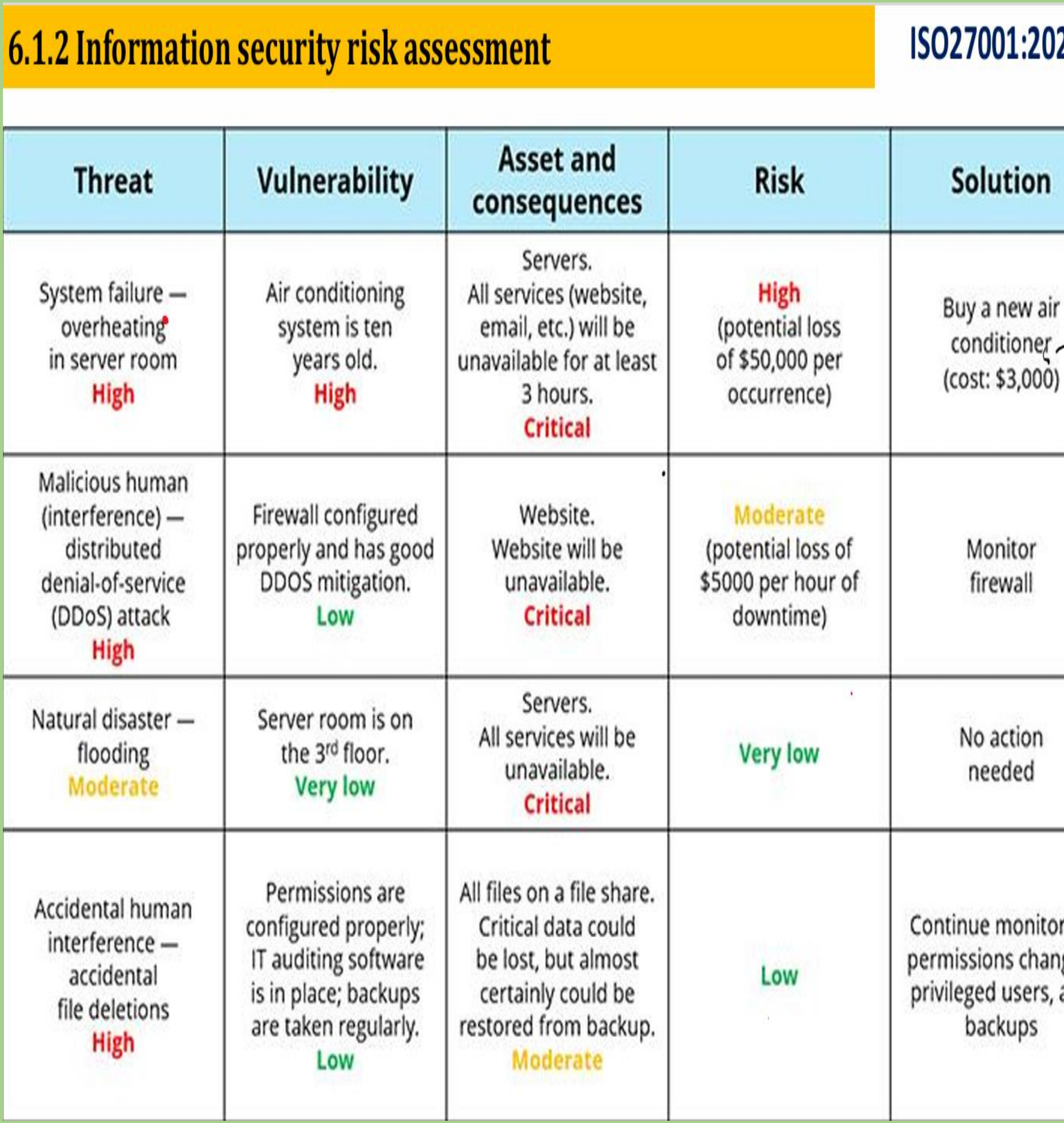
Risk Assessment - Vulnerability(s) considered along with existing controls before the Risk Evaluation done to understand the current baseline – before mitigating the same

Overall process of risk identification, risk analysis and risk evaluation and risk mitigation (controls) for the situations & their causes, which contribute to business disruption – C, I & A Separately

Very likely	Medium 2	High 3	Extreme 5
Likely	Low 1	Medium 2	High 3
Unlikely	Low 1	Low 1	Medium 2
What is the chance it will happen?	Minor	Moderate	Major

Impact

Below is a sample of risk Assessment

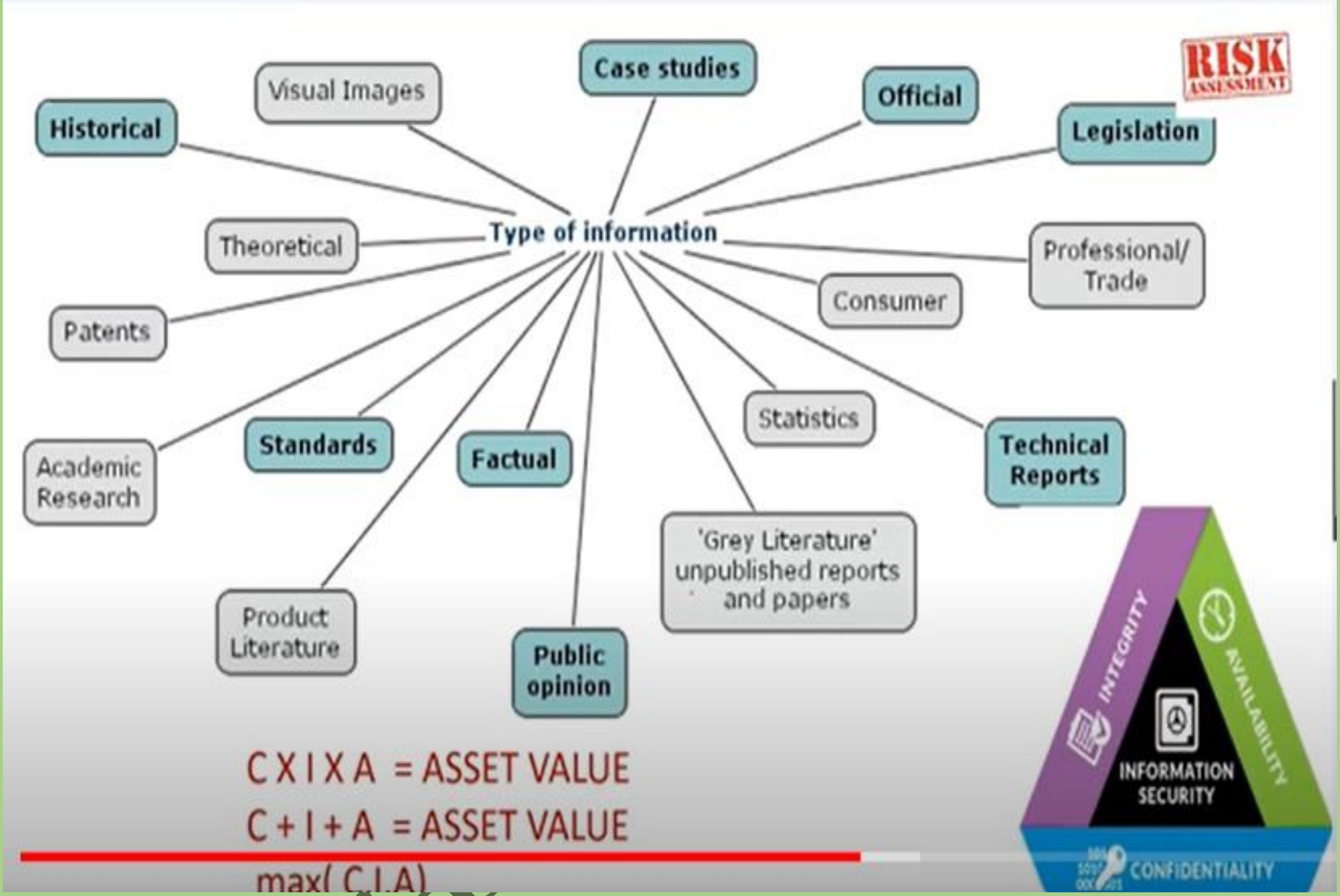


6.1.2 Information security risk assessment

ISO27001:202

Threat	Vulnerability	Asset and consequences	Risk	Solution
System failure — overheating in server room High	Air conditioning system is ten years old. High	Servers. All services (website, email, etc.) will be unavailable for at least 3 hours. Critical	High (potential loss of $50,000 per occurrence)	Buy a new air conditioner (cost: $3,000)
Malicious human (interference) — distributed denial-of-service (DDoS) attack High	Firewall configured properly and has good DDOS mitigation. Low	Website. Website will be unavailable. Critical	Moderate (potential loss of $5000 per hour of downtime)	Monitor firewall
Natural disaster — flooding Moderate	Server room is on the 3rd floor. Very low	Servers. All services will be unavailable. Critical	Very low	No action needed
Accidental human interference — accidental file deletions High	Permissions are configured properly; IT auditing software is in place; backups are taken regularly. Low	All files on a file share. Critical data could be lost, but almost certainly could be restored from backup. Moderate	Low	Continue monitor permissions chan privileged users, a backups

Below is a sample of Assets:



C X I X A = ASSET VALUE

C + I + A = ASSET VALUE

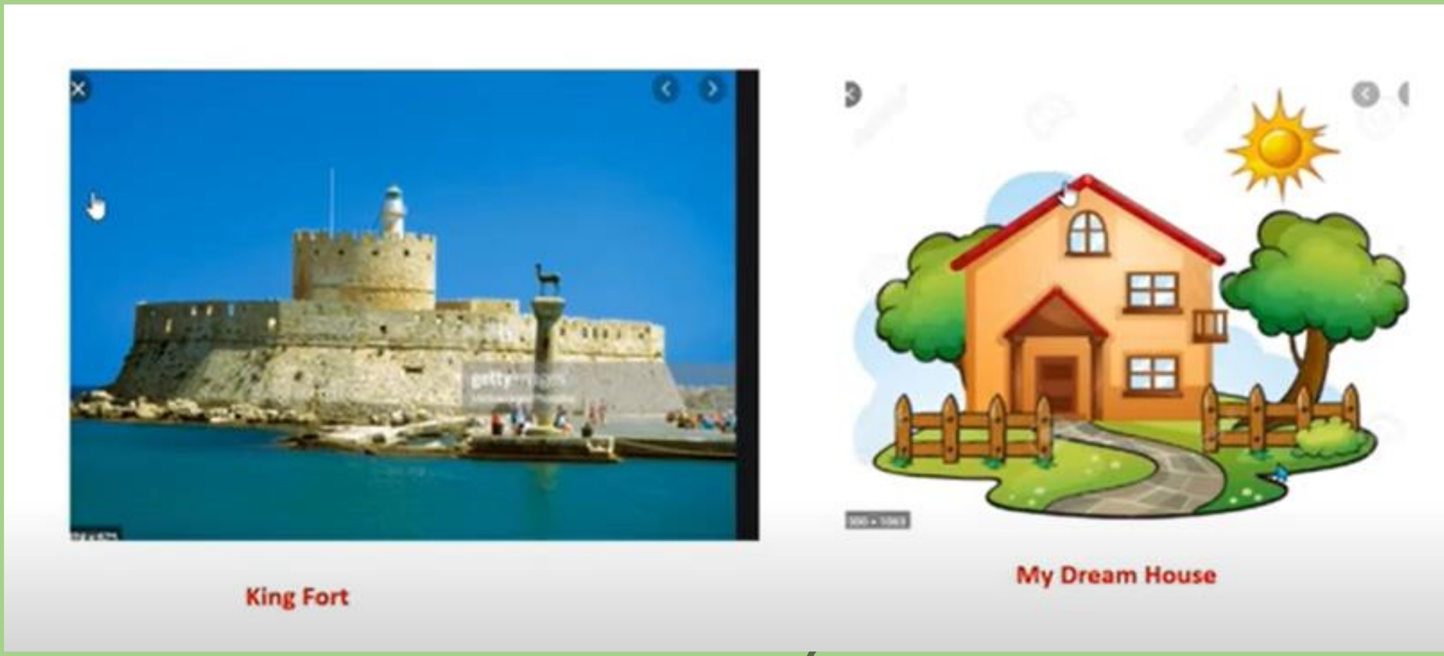
max(C,I,A)

Exercise 12

- Write your risk Assessment Methodology
- Considering your company as a case study for ISO 27001:2022 implementation
- It might be either Asset-based or issue-based risk Assessment
- You can only do this exercise after making a list of assets (inventory): Exercise – 13

Practical Illustration of doing Risk Assessment

Risk Assessment - It is the process of identifying vulnerabilities and threats to the information resources used by the organization in achieving business objectives and deciding what controls, if any to reduce the risk to an acceptable level, based on the information resource to the organization



King Fort

- Built on a height
- Has a watch tower - surveillance
- Water with no gates: Creatures
- Walls: Someone can attack before you attack

Dream House

- Passage is clear
- Windows are glass made of glass - can be broken
- No signs of CCTV cameras
- The overall objective is to safeguard the assets (Information)
- Determine the Asset (information value) via critical Asset values

- C + I + A = Asset Value
- C x I x A = Asset Value
- max (CIA)
- Don't use the same formula (stick to one)

Exercise 13:

- Make a List of Information Asset (Inventory)
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 14:

- Make a list of risks / issues as per the organization
- Considering your company as a case study for ISO 27001:2022 implementation

Exercise 15:

- List down Information security objectives of your organization
- Considering your company as a case study for ISO 27001:2022 implementation

Services that you can offer:

We Provide exclusive Risk Assessment Services to assist you with implementation of Information Security Practices into your organization

Risk Advisory Services

Third Party Risk Assessment

Gap Assessment Services

Cyber Security Audit & Consultancy Services