INFOCUS-IT

ISMS Part-II

ISO 27001

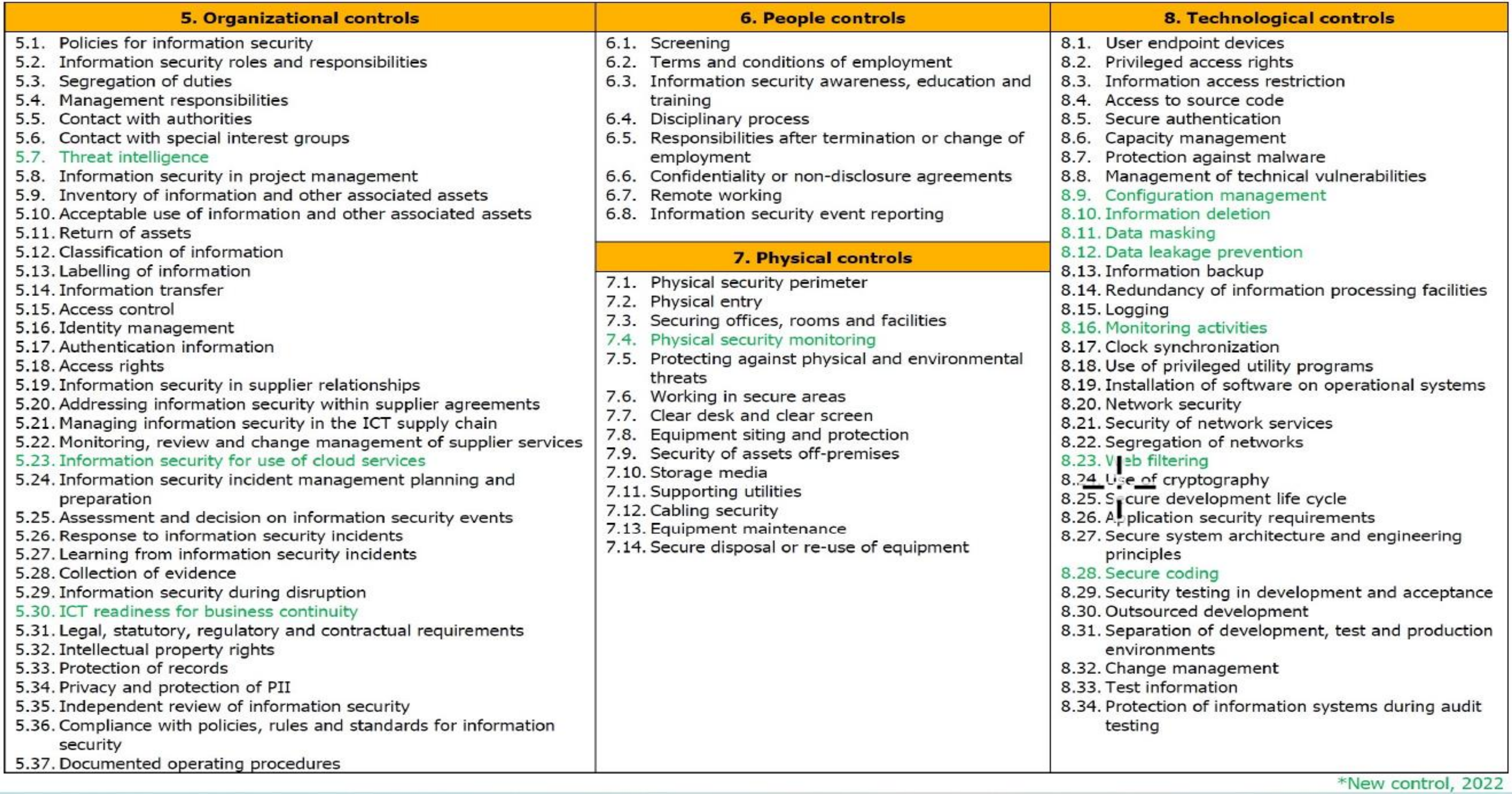
Ver.2022

ISO27001:2022 lead Implementor Course

By Jagbir Singh | jagbir@infocus-it.com

MTech(CS) | LLB |CISA | ISO27001LA |ISO22301LA|CEH|CHFI

Exercise A – Start here



5. Organizational controls

5.1. Policies for information security
5.2. Information security roles and responsibilities
5.3. Segregation of duties
5.4. Management responsibilities
5.5. Contact with authorities
5.6. Contact with special interest groups
5.7. Threat intelligence
5.8. Information security in project management
5.9. Inventory of information and other associated assets
5.10. Acceptable use of information and other associated assets
5.11. Return of assets
5.12. Classification of information
5.13. Labelling of information
5.14. Information transfer
5.15. Access control
5.16. Identity management
5.17. Authentication information
5.18. Access rights
5.19. Information security in supplier relationships
5.20. Addressing information security within supplier agreements
5.21. Managing information security in the ICT supply chain
5.22. Monitoring, review and change management of supplier services
5.23. Information security for use of cloud services
5.24. Information security incident management planning and preparation
5.25. Assessment and decision on information security events
5.26. Response to information security incidents
5.27. Learning from information security incidents
5.28. Collection of evidence
5.29. Information security during disruption
5.30. ICT readiness for business continuity
5.31. Legal, statutory, regulatory and contractual requirements
5.32. Intellectual property rights
5.33. Protection of records
5.34. Privacy and protection of PII
5.35. Independent review of information security
5.36. Compliance with policies, rules and standards for information security
5.37. Documented operating procedures

6. People controls

6.1. Screening
6.2. Terms and conditions of employment
6.3. Information security awareness, education and training
6.4. Disciplinary process
6.5. Responsibilities after termination or change of employment
6.6. Confidentiality or non-disclosure agreements
6.7. Remote working
6.8. Information security event reporting

7. Physical controls

7.1. Physical security perimeter
7.2. Physical entry
7.3. Securing offices, rooms and facilities
7.4. Physical security monitoring
7.5. Protecting against physical and environmental threats
7.6. Working in secure areas
7.7. Clear desk and clear screen
7.8. Equipment siting and protection
7.9. Security of assets off-premises
7.10. Storage media
7.11. Supporting utilities
7.12. Cabling security
7.13. Equipment maintenance
7.14. Secure disposal or re-use of equipment

8. Technological controls

8.1. User endpoint devices
8.2. Privileged access rights
8.3. Information access restriction
8.4. Access to source code
8.5. Secure authentication
8.6. Capacity management
8.7. Protection against malware
8.8. Management of technical vulnerabilities
8.9. Configuration management
8.10. Information deletion
8.11. Data masking
8.12. Data leakage prevention
8.13. Information backup
8.14. Redundancy of information processing facilities
8.15. Logging
8.16. Monitoring activities
8.17. Clock synchronization
8.18. Use of privileged utility programs
8.19. Installation of software on operational systems
8.20. Network security
8.21. Security of network services
8.22. Segregation of networks
8.23. Web filtering
8.24. Use of cryptography
8.25. Secure development life cycle
8.26. Application security requirements
8.27. Secure system architecture and engineering principles
8.28. Secure coding
8.29. Security testing in development and acceptance
8.30. Outsourced development
8.31. Separation of development, test and production environments
8.32. Change management
8.33. Test information
8.34. Protection of information systems during audit testing

*New control, 2022

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

ISO27001:2022

1. **Introduction** – describes what information security is and why an organization should manage risks.
2. **Scope** – covers high-level requirements for an ISMS to apply to all types or organizations.
3. **Normative References** – explains the relationship between ISO 27000 and 27001 standards.
4. **Terms and Definitions** – covers the complex terminology that is used within the standard.
5. **Context of the Organization** – explains what stakeholders should be involved in the creation and maintenance of the ISMS.
6. **Leadership** – describes how leaders within the organization should commit to ISMS policies and procedures.
7. **Planning** – covers an outline of how risk management should be planned across the organization.
8. **Support** – describes how to raise awareness about information security and assign responsibilities.
9. **Operation** – covers how risks should be managed and how documentation should be performed to meet audit standards.
10. **Performance Evaluation** – provides guidelines on how to monitor and measure the performance of the ISMS.
11. **Improvement** – explains how the ISMS should be continually updated and improved, especially following audits.
12. **Reference Control Objectives and Controls** – provides an annex detailing the individual elements of an audit.

ISO27001:2022

Clause -5 | Leadership

5.1 Leadership and commitment

5.2 Policy

5.3 Organizational roles, responsibilities and authorities

Clause -5 | Leadership

ISO27001:2022

5.1 Leadership and commitment

Top management shall demonstrate leadership and commitment 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; and

h) supporting other relevant management roles to demonstrate their leadership as it applies to their areas of responsibility.

Clause -5 | Leadership

ISO27001:2022

5.2 Policy

Top management shall establish an information security policy that:

a) is appropriate to the purpose of the organization;

b) includes information security objectives (see 6.2) or provides the framework for setting information

security objectives;

c) includes a commitment to satisfy applicable requirements related to information security;

d) includes a commitment to continual improvement of the information security management system.

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.

Clause -5 | Leadership

5.2 Policy

Exercise-6	Write your Information security policy

Sample Information security policy

https://infocus-it.com/information-security-policy/

Clause -5 | Leadership

ISO27001:2022

5.3Organizational roles, responsibilities and authorities

Top management shall ensure that the responsibilities and authorities for roles relevant to information security are assigned and communicated within the organization.

Top management shall assign the responsibility and authority for:

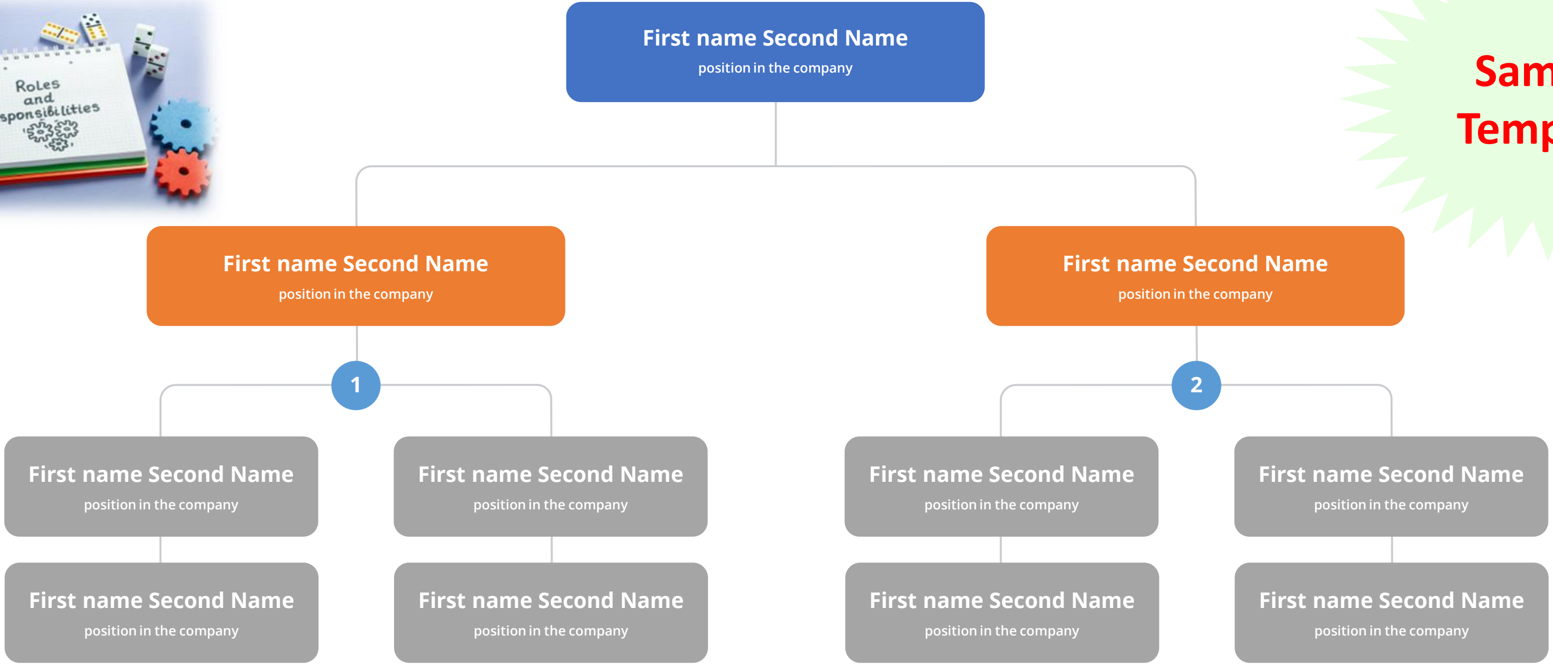
a) ensuring that the information security management system conforms to the requirements of this document;

b) reporting on the performance of the information security management system to top management.

Clause -5 | Leadership

5.3Organizational roles, responsibilities and authorities

Sample Template



Clause -5 | Leadership

5.3Organizational roles, responsibilities and authorities

Exercise -7

Draw Organization chart as per your company structure (only to cover information security team & concerned team) you can seek help from HR Dept. for Roles and responsibilities

Exercise -8

Define Roles and responsibilities as per the organization chart in exercise -7

ISO27001:2022

Clause -6 | Planning

6.1 Actions to address risks and opportunities

6.1.2 Information security risk assessment

6.2 Information security objectives and planning to achieve them

Clause -6 | Planning

6.1 Actions to address risks and opportunities

When planning for the information security management system, the organization shall consider the issues referred to in 4.1 and the requirements referred to in 4.2 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;

c) achieve continual improvement.

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.

ISO27001:2022

Clause -6 | Planning

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;

2) Assessment - a) identify the risk owners; b) assess the potential consequences that would result if the risks identified were to materialize;

c) assess the realistic likelihood of the occurrence of the risks identified 3) determine the levels of risk;

b) evaluates the information security risks:

1) compare the results of risk analysis with the risk criteria.

2) prioritize the analysed risks for risk treatment.

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

Clause -6 | Planning

ISO27001:2022

6.2 Information security objectives and planning to achieve them

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 monitored; e) be communicated; f) be updated as appropriate; g) be available as documented information.

The organization shall retain documented information on the information security objectives.

When planning how to achieve its information security objectives, the organization shall determine:

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

Clause -6 | Planning

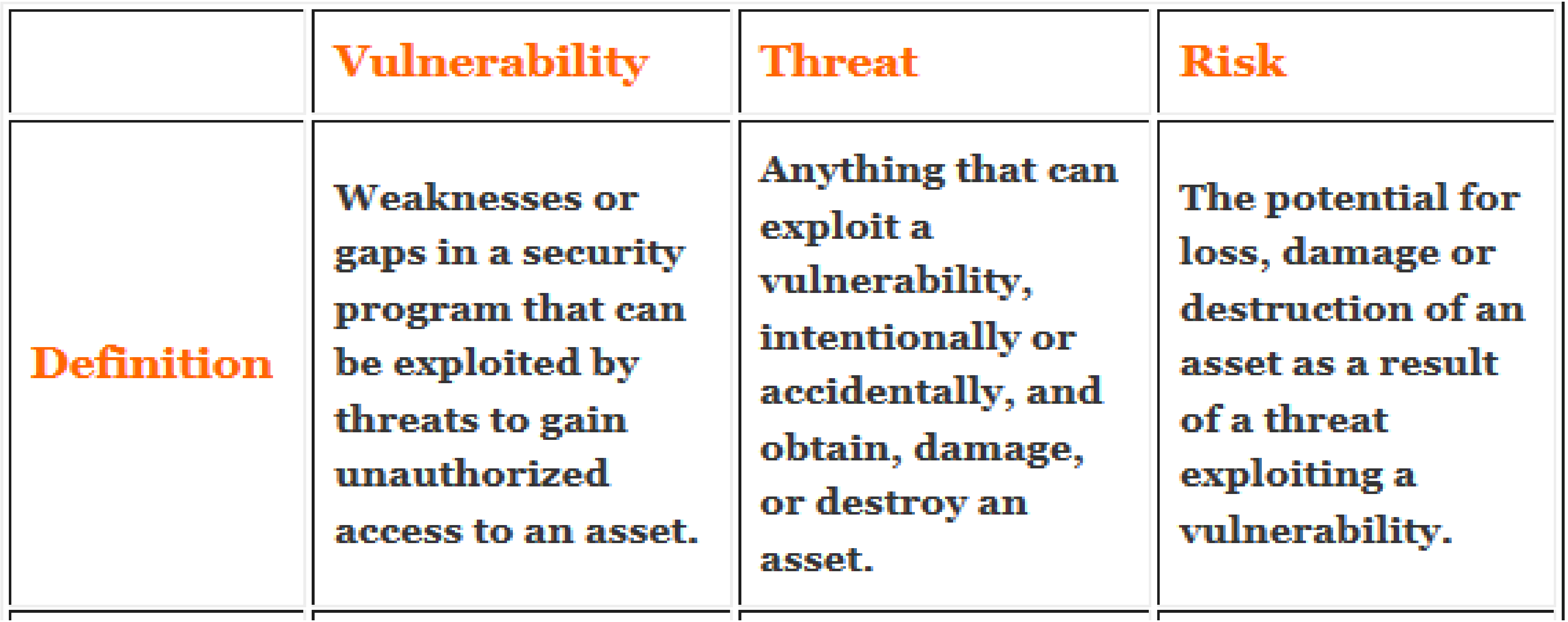
ISO27001:2022

6.2 Information security objectives and planning to achieve them

Exercise-12	List down information security objectives of your organization

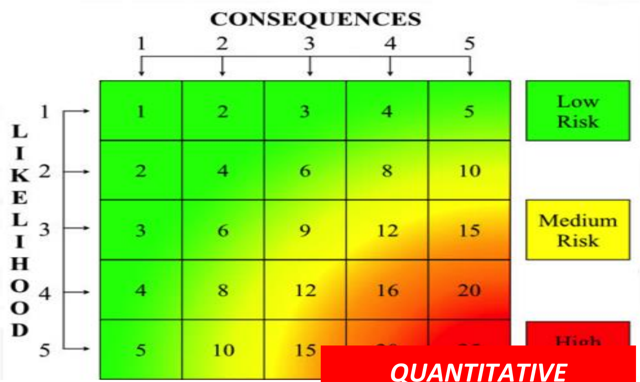
Clause -6 | Planning

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.

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

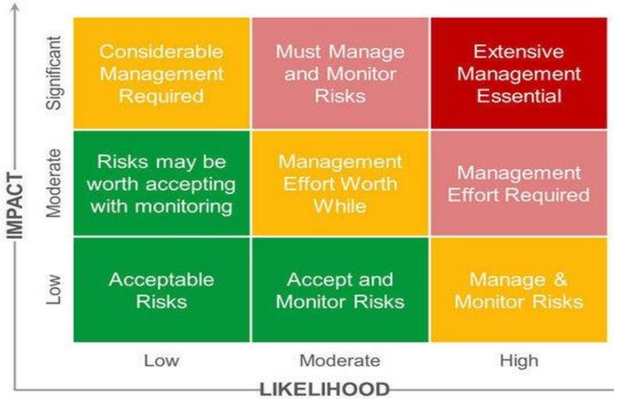


CONSEQUENCES → LIKELIHOOD ↓	1	2	3	4	5
1	1	2	3	4	5
2	2	4	6	8	10
3	3	6	9	12	15
4	4	8	12	16	20
5	5	10	15		

Low Risk
Medium Risk
High

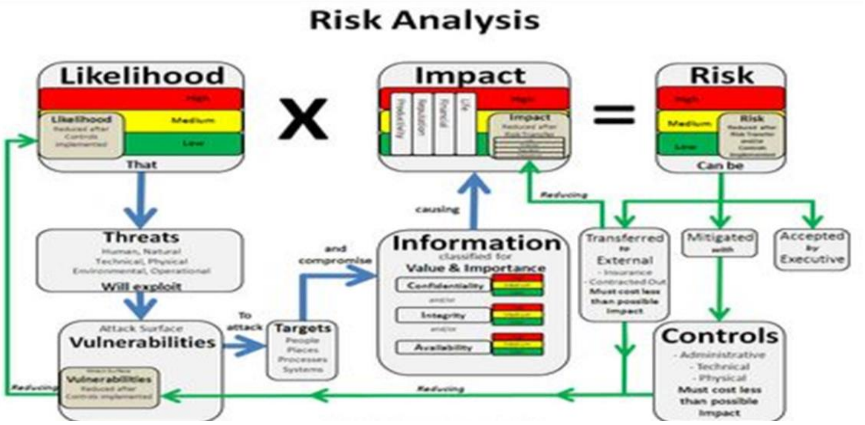
Risk Assessment

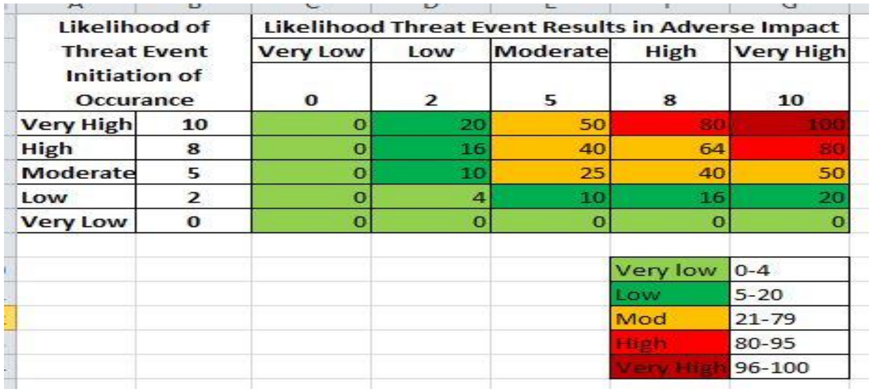
QUANTITATIVE
QUALITATIVE



IMPACT / LIKELIHOOD	Low	Moderate	High
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

COMBINED
Qualitative + Quantitative





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

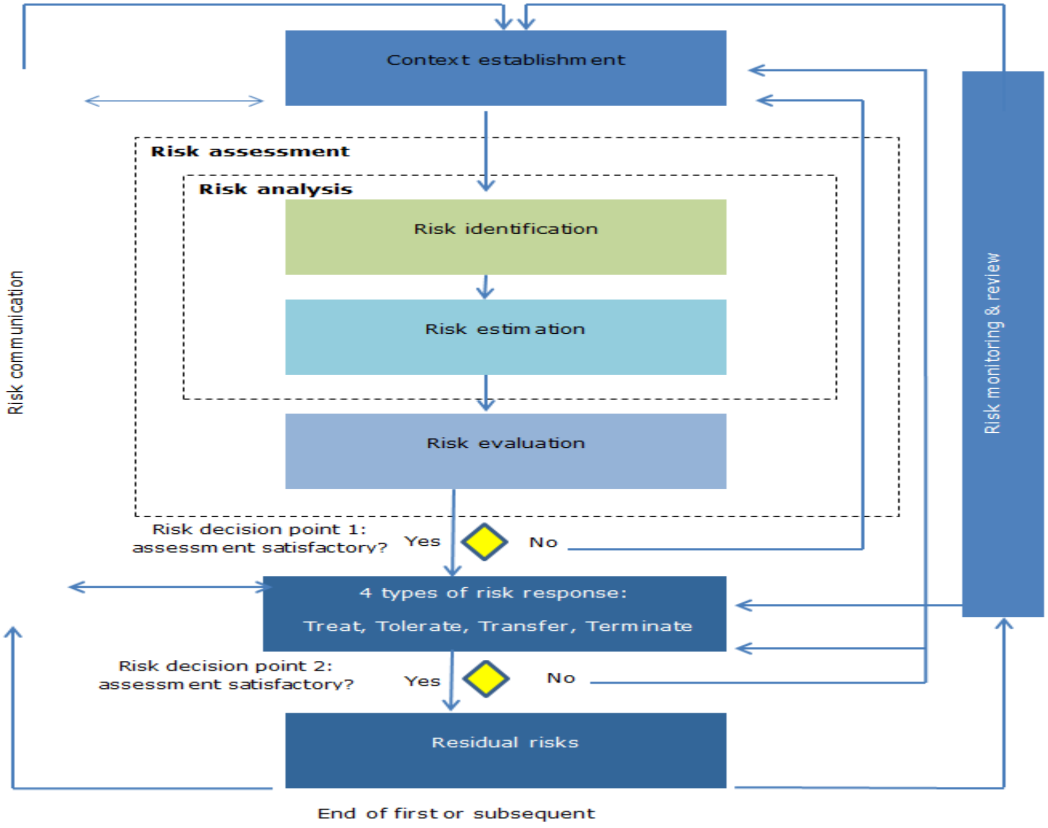
Very low	0-4
Low	5-20
Mod	21-79
High	80-95
Very High	96-100

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

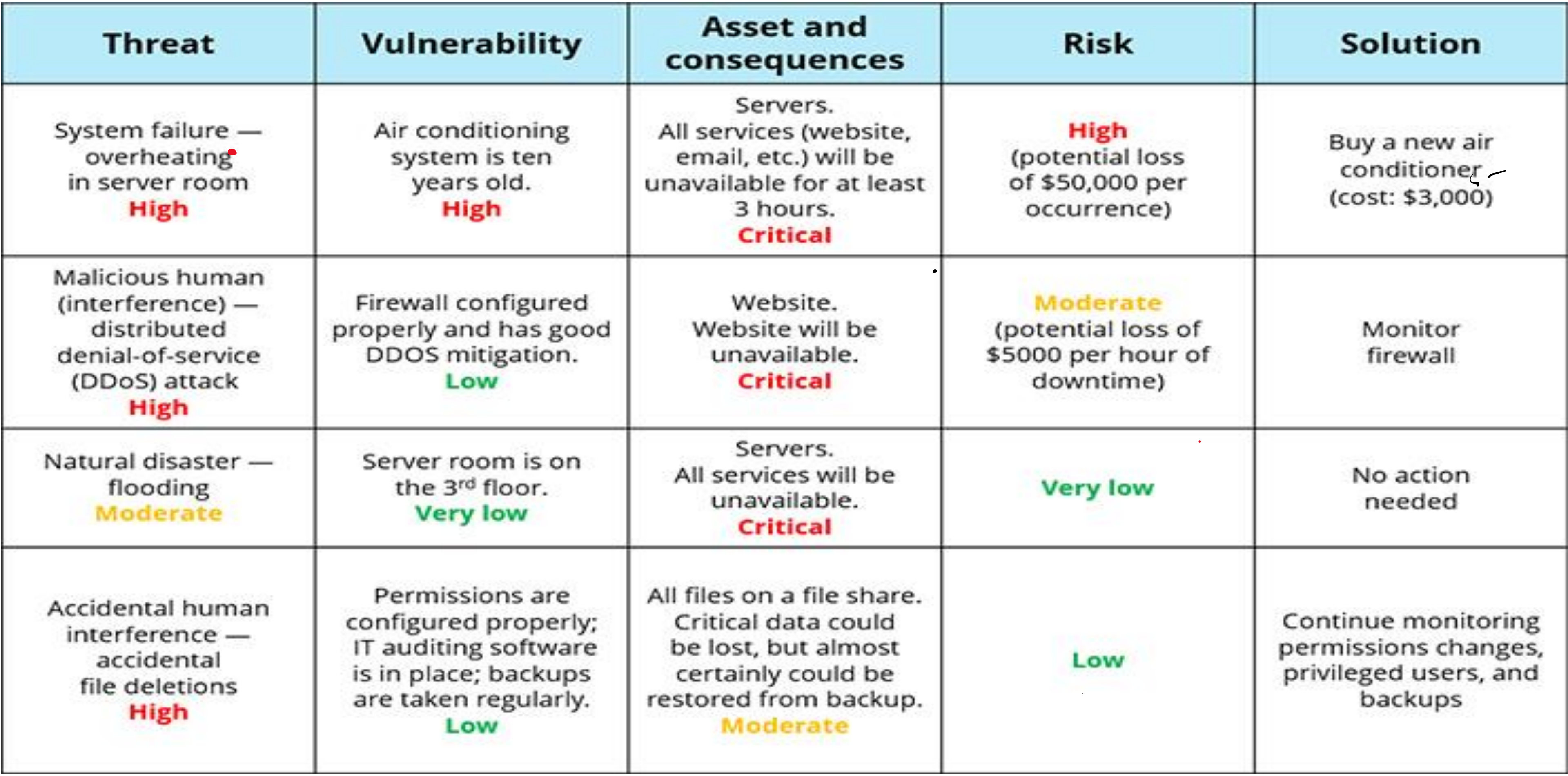
Overall process of risk identification, risk analysis and risk evaluation and risk mitigation (controls) for the situations & their causes, which contribute to business disruption – C, I & A Separately

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

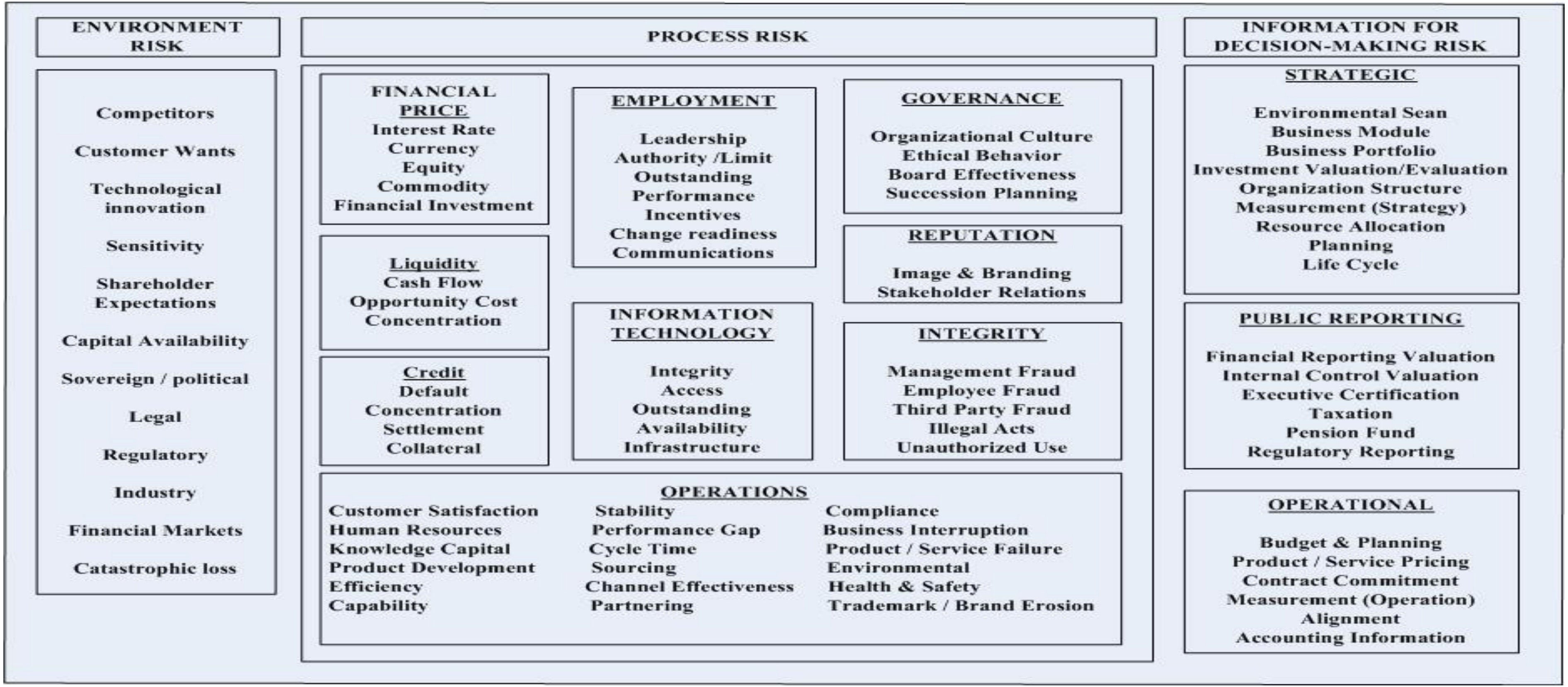

Context establishment
Risk assessment
Risk analysis
Risk identification
Risk estimation
Risk evaluation
Risk decision point 1: assessment satisfactory?
Yes
No
4 types of risk response:
Treat, Tolerate, Transfer, Terminate
Risk decision point 2: assessment satisfactory?
Yes
No
Residual risks
End of first or subsequent
Risk communication
Risk monitoring & review

6.1.2 Information security risk assessment



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 monitoring permissions changes, privileged users, and backups

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

Clause -6 | Planning

6.1.2 Information security risk assessment

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

How Can we Help you

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

INFOCUS-IT | support@infocus-it.com | 91-8178210903