Standard Practice- Risk Management

Owner Name: Process Excellence Team (PeX)

Version: 4.0

neurealm

Document History

Version	Date	Summary of Changes	Author	Approved By
2.00	4/5/2020	Revised version 2.0 released	Rama Vani Periasamy	Sekar T Security Council
3.00	30/5/2023	Updated with new Risk Standards followed in GAVS	Shalot Leely M	Sekar T
3.01	22/02/2024	Updated with PCI- DSS 4.0 requirement	Shalot Leely M	Sekar T
4.0	13-05-2025	Organization name change & updated in Neurealm format	Shalot Leely M	Ambrish S

Contents

Section A: Introduction

1. Overview

The purpose of this document is to provide a detailed overview of the Enterprise Risk management process. Enterprise risk management (ERM) is the processes and methods used by enterprise to manage risks and take advantage of opportunities related to the achievement of their objectives. Typically, ERM covers various risk types, including compliance, cybersecurity ("cyber information security"), financial, legal, legislative, operational, reputational, safety, privacy, supply chains and strategic. Enterprise Risk Management (ERM) and are those risks which if they occur could lead to losses that affect the entire enterprise in a drastic and adverse way.

ERM provides a framework for identifying events or circumstances relevant to the organization's objectives that has potential threats and opportunities, assessing them in terms of likelihood and magnitude of impact, determining a response strategy, and monitoring progress of mitigations. By identifying and proactively addressing risks and opportunities, the enterprise protects and creates value for the interested parties, including board of directors, investors, employees, customers, regulators, and society overall.

Organization adopt an ERM framework to increase risk awareness and transparency, improve risk management strategies, and align risks to each organization's risk tolerance and risk thresholds. Risk tolerance is the amount of risk an organization is willing to accept in relation to strategic objectives and the value to the enterprise.

Managing risk is based on the principles, framework and process outlined in this document, as illustrated in Figure 1. These components might already exist in full or in part within the organization, however, they might need to be adapted or improved so that managing risk is efficient, effective, and consistent. The components of the framework and the way in which they work together should be customized to the needs of the organization / engagement.

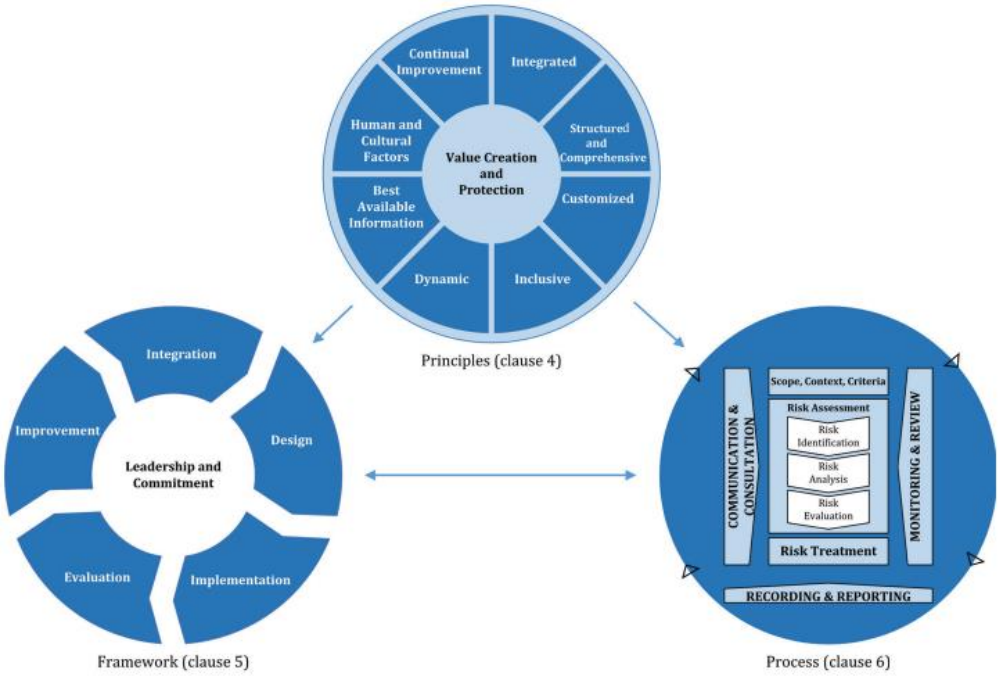


Figure 1 — Principles, framework and process

2. Principles

The purpose of risk management is the creation and protection of value. It improves performance, encourages innovation and supports the achievement of objectives. The principles outlined in Figure 2 provide guidance on the characteristics of effective and efficient risk management, communicating its value and explaining its intention and purpose. The principles are the foundation for managing risk and should be considered when establishing the organization's risk management framework and processes. These principles should enable an organization to manage the effects of uncertainty on its objectives.

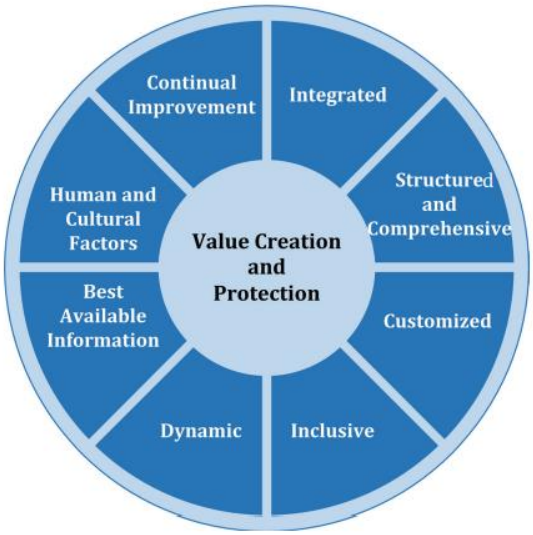


Figure 2 — Principles

Effective risk management requires the elements of Figure 2 and can be further explained as follows. a) Integrated Risk management is an integral part of all organizational activities.

b) Structured and comprehensive A structured and comprehensive approach to risk management contributes to consistent and comparable results.

c) Customized The risk management framework and process are customized and proportionate to the organization's external and internal context related to its objectives.

d) Inclusive Appropriate and timely involvement of stakeholders enables their knowledge, views and perceptions to be considered. This results in improved awareness and informed risk management.

e) Dynamic Risks can emerge, change or disappear as an organization's external and internal context changes. Risk management anticipates, detects, acknowledges and responds to those changes and events in an appropriate and timely manner.

f) Best available information

The inputs to risk management are based on historical and current information, as well as on future expectations. Risk management explicitly takes into account any limitations and uncertainties associated with such information and expectations. Information should be timely, clear and available to relevant stakeholders

g) Human and cultural factors Human behavior and culture significantly influence all aspects of risk management at each level and stage.

h) Continual improvement Risk management is continually improved through learning and experience

3. Process Objective

The primary objective of Risk Management Process is to identify, assess, control, monitor and communicate. This includes identification of risk, analyzing the impact of risk to the business, identifying threats, evaluating the vulnerability of each risk to those threats, and constant monitoring of threat parameters.

4. Scope

Scope refers to the boundaries or extent of influence to which risk management applies. This section provides the scope for risk management regarding the process itself, Customers, Service Providers and IT Service and Service Components and environment.
The scope of the risk management process covers the design, implementation, measurement, management and improvement of IT service and component availability. Risk management commences as soon as the availability requirements for an IT service are clear enough to be articulated.

5. Benefits

There are several qualitative and quantitative benefits that can be achieved, for both the IT Service Providers and the Customers, by implementing an effective and efficient Risk Management process.

6. Key Terms and Definitions

Risk :- According to ISO 31000, risk is the “effect of uncertainty on objectives” and an effect is a positive or negative deviation from what is expected.

Risk :- According to PMBOK, risk can be defined as an uncertain event or condition that results in a positive or negative effect on a project's objectives. Whereas, an issue can be defined as an event or condition that has already happened and has impacted or currently impacting the project objectives

Risk vs Opportunity :

A risk is a potential for a loss, An Opportunity is a potential for a gain. Most strategies and plans entail both risk and opportunity. As such both play a role in decision making, strategy formation and management

Risk Register:

The Risk Register is the database which keeps track of identified risks and subsequent countermeasures. In ITIL, Risk Register is also termed as the Risk Log.

Business Impact and Risk Analysis:

Business Impact Analysis (BIA) and Risk Analysis are concepts associated with ITIL Risk Management & IT Service Continuity Management. Their goal is to identify those risks that are to be managed through risk mitigation measures.

Process and Asset Valuation:

An estimated value of a process, or other assets used in the business. This value is an important input for Risk Analysis.

Risk Management Policy:

This Policy Document describes and communicates the organization's approach to managing risk.
Most importantly, it defines how risk is detected and who oversees specific risk management duties.

Risk Owner:

Risk Owner is the person who would be responsible for the implementation of risk mitigation measures & ongoing maintenance of it.

Risk Acceptance Criteria: A list of minimum requirements that a service or service component must meet for it to be acceptable to the interested parties.

Section B: Roles and Responsibilities

1. User Roles and Functions

The responsibilities of various user roles in Availability Management are listed as follows:

Roles	Responsibilities
Risk Owner	The Risk Owner to identify, assess, and control risks. This includes the: analysis of criticality of IT assets for the business (includes PCI-DSS requirement Assets) analysis of possible threats for separate IT assets evaluation of occurrence probability for different threats evaluation of occurrence effects for different threats definition of risk monitoring procedures definition of risk avoidance activities

2. RACI Matrix

The following RACI chart outlines which positions are Responsible, Accountable, Consulted, and Informed for each service desk process.

Activities	Risk Owner	Other roles involved
Risk Management Support	A,R	-
Business Impact and Risk Analysis	A,R	R
Assessment of Required Risk Mitigation	A,R	-
Risk Monitoring	A,R	-

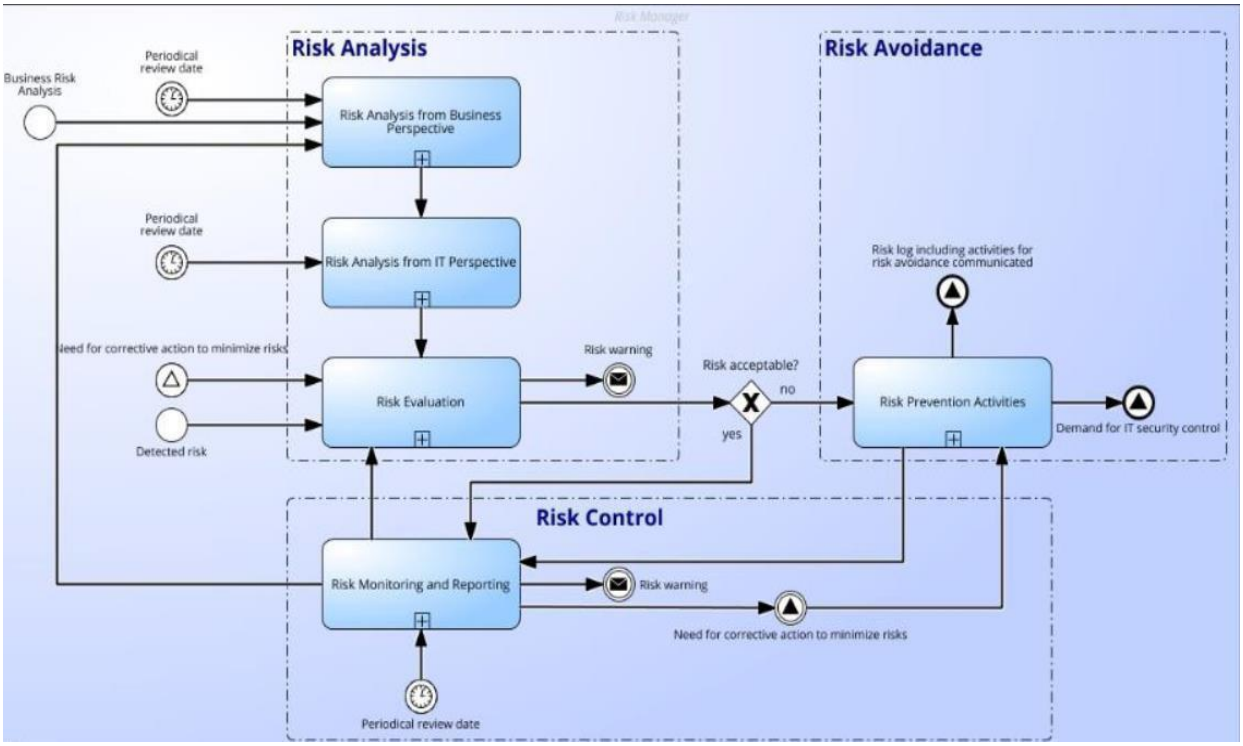
Risk Owner works with Availability Manager, IT Service Continuity Manager, Information Security Manager, Compliance Manager, and Supplier Manager

Section C: Process Flow

1. Risk Management Process flow

The main objectives of ITIL's risk management process are to identify, assess, and control risks that have been identified using a risk matrix. This may involve analyzing business assets, threats to those assets, monitoring threat parameters, and evaluating the business's vulnerability to those threats. There are several stages to ITIL risk management which are:

- Identify and characterize threats.
- Assess vulnerability of critical assets to specific threats
- Determine the probability of risks and their impact.
- Identify ways to reduce risks.
- Prioritize risk reduction measures.
- Continuously monitor risk factors



1.1 Risk Management Sub Process

As well as these stages alongside the risk matrix, there are also four principle sub-processes to the ITIL risk management framework:

1.1.1 Risk management support

It is the process of defining the roles and responsibilities of those involved in ITIL risk management. This sub-process details how to identify a risk, the level of risk that an organization is prepared to allow, and the duties carried out by IT employees.

The following activities are involved in the risk management support process.

Risk Identification: Risk identification is a methodical approach to ensure all significant activities within the organization have been identified and all risks flowing from those activities are defined.

Methods of identifying risks include:

•risk workshops

•stakeholder consultations

•benchmarking

•scenario or 'what if' analysis

•audits and assessments

•research methods (interviews, surveys, etc.)

•cause and effect diagrams.

Identified risks need to be displayed in a structured format, using a table to facilitate risk description and assessment.

Risk Assessment: Identified risks should be recorded in a risk Assessment in CSM portal. This can include the following information:

a unique identifier number, risk category, description of risk, the date the risk is identified ,Risk Owner and by whom.

Other possible data includes the likelihood of risk, consequences, interdependencies with other risks and a regulatory estimation.

Frequency of performing risk assessment:

Mandatory is quarterly and Recommended is monthly

1.1.2 Business impact and risk analysis

This step involves measuring the impact of risk to the organization and determining the probability and/or vulnerability of the risk occurring.

Risk Estimation: Risk estimation can be quantitative, semi-quantitative or qualitative in terms of likelihood of occurrence and possible consequences. Assessing the impact of each risk can be done using a variety of tools including:

- Probability & statistical inference
- scenario planning.
- simulations, including Monte Carlo spreadsheet simulation.
- decision trees.
- real option modelling.
- sensitivity analysis.
- risk mapping.
- SWOT or PESTELE analysis – Refer BMS Manual for PESTELE analysis approach.
- root cause analysis.
- cost benefit/risk benefit analysis
- FMEA (Failure Mode & Effect Analysis)
- Business continuity planning

Risk mapping is the most frequent example of how risks are assessed. Mapping involves a matrix of likelihood/probability and impact/consequences.

1.1.3 Assessment of required risk response

Determining the risk response measures required and allocating a Risk Owner to the identified risks. Responses to risk generally fall into the following categories:

- Risk avoidance: action is taken to halt the activities giving rise to risk, such as a product line, a geographical market, or a whole business unit.
- Risk reduction: action is taken to mitigate the risk of likelihood or impact or both, generally via

internal controls.

- Risk sharing or transfer: action is taken to transfer a portion of the risk through insurance, outsourcing or hedging.
- Risk acceptance: no action is taken if there is no likelihood or impact of the risk on the organization /interested parties. The following risk acceptance criteria are established

Risk Response/Treatment Strategy

Criteria for Approving Risk Assessments	
All Risk Assessments must be approved by the top management, either through Management Review or by documented approvals.	
Risk Appetite	
No	N/A - risk removed
Low	Acceptable risk and no further action required as the risk has been minimized and monitored as far as possible. Risks needs to be reviewed at least annually.
Moderate	Tolerable with further action required to mitigate risk or remove. Risk needs to be reviewed at least every 6 months.
High	Tolerable with further action required to mitigate risk or remove. Risk needs to be reviewed at least every 3 months.
Catastrophic	Unacceptable risk and urgent action required to mitigate or remove the risk. Risk needs to be reviewed monthly.

Consequences of the event on CIA (Confidentiality, Integrity, Availability) Guideline in qualitative words		
None	0	No consequences - for example the control has eliminated them
Insignificant	1	No visible impact to company reputation/customer satisfaction. No potential impact on market share/brand values
Minor	2	Potential impact on market share/brand values. Internal control significant deficiency
Significant	3	Visible reputation/satisfaction impact. Reputation and brand value will be affected in the short term. Internal control material weakness
Major	4	Visible adverse brand value/market share publicity. Key alliances are threatened. Loss of key customers. SEC investigation or matter. Financial restatement.
Critical	5	Major company reputation impact. Revocation of licenses or regulatory registrations. Major customer satisfaction impact. Inability to service customers. Loss of major investor/street confidence

Likelihood Value				
Guideline in qualitative words			Probability	Frequency
Impossible	0	The event is impossible - for example the risk source has been removed or activity has been stopped	0%	will not happen
Rare	1	The possibility of occurrence is so low. These are exceptional circumstances or it may never happen	<1%	it may never happen
Remote	2	Unlikely to happen	2-10%	doubt that it occurs
Moderate	3	Believe it could occur	11-50%	is at least 1 per year
Likely	4	May occur sometimes	51-90%	occasionally during a year
Frequent	5	Known to occur. Almost certain.	>90%	several times in a year

Risk Matrix

Risk Rating Matrix		Consequences					
		Critical	Major	Significant	Minor	Insignificant	None
Likelihood		5	4	3	2	1	0
Frequent	5	Catastrophic	Catastrophic	High	High	Moderate	No
Likely	4	Catastrophic	High	High	Moderate	Low	No
Moderate	3	High	High	Moderate	Moderate	Low	No
Remote	2	High	Moderate	Moderate	Low	Low	No
Rare	1	Moderate	Low	Low	Low	Low	No
Impossible	0	No	No	No	No	No	No

Avoid

Trasfer / Share

Share/Trasfer

Reduce

Accept

Accept

Risk Rating Matrix:

The risk score is the result of the analysis, calculated by multiplying the Risk Likelihood by Risk Consequence.

It's the quantifiable number that allows to quickly and confidently make decisions regarding risks.

RISK = Likelihood x Consequences

Risk Rating Matrix		Consequences					
		Critical	Major	Significant	Minor	Insignificant	None
Likelihood		5	4	3	2	1	0
Frequent	5	25	20	15	10	5	No
Likely	4	20	16	12	8	4	No
Moderate	3	15	12	9	6	3	No
Remote	2	10	8	6	4	2	No
Rare	1	5	4	3	2	1	No
Impossible	0	No	No	No	No	No	No

1.1.4 Risk monitoring & reporting

This step involves continuously monitoring the progress of risk mitigation measures and countermeasures that have been implemented. This includes taking action to correct where necessary. Risk monitoring also include reporting & communication.

Different levels within an organization need different information from the risk management process.

The higher management should:

- know about the most significant risks facing the organization,
- know the possible effects on shareholder value of deviations to expected performance ranges.
- ensure appropriate levels of awareness throughout the organization.
- know how the organization will manage a crisis.
- know the importance of stakeholder confidence in the organization.
- know how to manage communications with the investment community where applicable assured that the risk management process is working effectively.
- publish a clear risk management policy covering risk management philosophy and responsibilities The different types of risk reporting are:
    1. Project Risk Reporting - Project risk reporting is at the lowest level in the project risk hierarchy. This is carried out by each project manager and the appropriate members of the project team. Project-level reporting covers risks that are relevant to the scope of the project work, and external factors that may affect the project in some way.
    2. Program Risk Reporting - Program-level risks are those that relate to:
        a. A project within the program where the risk is significant enough to need to be escalated to the program manager

b. Overlaps or dependencies between projects within the program

3. The program overall, and do not naturally link back to a specific project.

- Portfolio Risk Reporting - Portfolio-level risk reporting is a way of showing the aggregated risk profile for all the projects and programs in the portfolio. The major risks per program (or per project, for those projects that do not form part of a program) are drawn together and presented in a way that makes it easy to see an overall summary.
- Business Risk Reporting - Some businesses include operational activity in the scope of the portfolio, so would not have a need for this level of reporting. However, it is common to see projects managed across the organization with a portfolio approach, and operational work falling outside that.
- Information security reporting :- Risks identified on the product / services / deliverables committed to customer / third parties and internal & external issues will be reported by SOC function and respective customer success manager.
- Health & Safety risk reporting :- OHS function (a.c.a HSE) will be reporting the OHS related Hazards, Incidents and Risks to the HSE Head and Quality council meet where Leadership team present and customer success managers

Section D: Governance and Process Controls

1. Key Performance Indicators & Critical Success Factors

The following lists key performance indicators (KPIs) &CSFs that have been selected for tracking the success of the Risk Management process.

Critical Success Factors	key performance indicators
Knowledge of Risks	● Rate of services with analysed risks within the risk log in %
Risk Avoidance	● Rate of services with defined activities to avoid risk occurr risk log in %
Effectivity of Risk Management	● Number of occurred known risks in absolute figures

	• Number of occurred previously not known risks in absolute figures • Number of incidents due to known risks in absolute figures • Number of incidents due to previously not known risks in absolute figures • Service downtimes due to occurred known risks in hours • Service downtimes due to previously not known risks in hours • Consequential costs of occurred known risks in $ • Consequential costs of occurred previously not known risks in $
No. of OHS Risks with severity rating	• No. of risks identified in the OHS with various severity & impact
No. of Information Security Risks with category	• No. of risks identified in the Info.Sec with various severity & impact

2. Reports

The following table lists the Management reports that help identify trends and allow review of the health of the process. The acid test of the relevance of a report is to have a sound answer to the question, “What decisions is this report helping management to make?”

Communicating with project stakeholders by means of project risk reports can be a critical driving force that lets undertake adequate risk management and achieve project outcomes according to expectations.

A risk report is a summary of project risks and opportunities, the latest status of treatment actions, and an indication of trends in the incidence of risks. The following items serve as the basis for generating project risk status reports:

- The risk register and the supporting risk treatment action plan
- Work performance data reviews
- Project schedule progress
- Status of project deliverables produced

3. Escalation Matrix

Escalation matrix allows you to notify the right stakeholders in the event of critical issues. You can notify the right people at the right time about critical activities based on the escalation matrix. The escalation matrix is time zone specific and can be available 24X7.

Please find the link to the escalation matrix template https://mygavs.gavstech.com/ims/

Section E: ITIL Inter-relationships and Best Practices

1. Relationships with other ITIL Processes

ITIL describes an integrated set of processes which, collectively, describe an overall approach or framework to service management These interdependencies for Risk Management process are described below.

1.1. Change Management

Change Management helps to reduce risk and the potential negative impacts and the risks associated with the undesirable outcomes.

Refer to the Change Management Process here - https://mygavs.gavstech.com/ims/

1.2. Availability Management

Availability management focuses on the reliability & continuity, thereby putting in place an alternate solution to continue services & reduce risk.

Refer to the Availability Management Process here - https://mygavs.gavstech.com/ims/

1.3. IT service continuity management

Risk management works collaboratively with this process on the assessment of business impact and risk and the provision of resilience, fail-over and recovery mechanisms.

1.4. Problem Management

Problem Management proposes solutions to the risk management by its proactive & reactive techniques and its goal to reduce service outages and reduce risks

Refer to the Problem Management Process here - https://mygavs.gavstech.com/ims

Section F:

Appendix - 1 – Templates & References

1. Templates

The supporting documents and the templates in Risk Management are available in MyGAVS and corresponding links are listed,

2. References

Document Name	Templates
Risk Management Plan	https://mygavs.gavstech.com/ims/
Risk Register	https://mygavs.gavstech.com/ims/ https://csm.gavstech.com – Risk Tracker feature

Model / Standard	Process Area reference / ISO Clause(s) no.
ISO 9001:2015	6.1 – Actions to address risks and opportunities
ISO 27001:2022	6.1 – Actions to address risks and opportunities
ISO 20000-1:2018	6.1 – Actions to address risks and opportunities
ISO 45001 :2018	6.1 – Actions to address risks and opportunities
ISO 31000	Guideline for Risk Management

Appendix - 2 - HIPAA Risk Assessment Check-list

Physical Safeguards
Office Access

Is there a security guard or access control system to control access to the office?
Are restricted office areas secured with locks or key card entry?
Are all vendors escorted while visiting areas of the office?
Is there a formal document retention and disposal policy for protected health information (e-PHI)?
Does the office have access to and use cross-cut shredders for convenient disposal of paper records? Alter the office contract with off-site shredding services?
How does the office staff dispose of electronic records (e.g., CDs, DVDs, hard drives)?
Is there an exit interview or process to ensure return or destruction of all PHI upon termination/leave/resig personnel?
Workstations and Remote/Mobile Device Access
Are office workstations (i.e., computers) restricted to office personnel?
Is there an on-site server that stores PHI for the office? If so, is the server area locked or accessible only by employees?
Does the office use a cloud-based service or off-site server to store e-PHI for the office?
Does the office dispose of or recycle old computers/hard drives/fax machines? Is the information containe computers/hard drives wiped clean before disposal or recycling?
Do office workstations/laptops use unique login/user names for each individual?
Do office workstations require passwords?
Emergency/Contingency Plans
Is there a plan or service in place for back-up and recovery of PHI in the event of an emergency or disaster?
Technical Safeguards
Security and Encryption
Do office workstations all have anti-virus software and use firewalls?
Is the anti-virus software regularly updated?
How complex are office workstation passwords?
How often are workstation passwords required to be changed?
Do office workstations time out and log out automatically after a period of inactivity?
Mobile Access

Does the office use laptops/tablets/mobile devices/flash drives to access office e-mails or PHI?
Are the laptops/tablets/mobile devices secured with password protection? Are flash drives secured with er
Does the office have a method to track workstation access by office personnel?
Does the office have the ability to terminate remote access to office workstations if laptops/tablets/mobile stolen or lost?
Does the office have the ability to remotely wipe office data and e-PHI from lost or stolen laptops/tablets/r
Does the office send e-mails with PHI to patients? Are e-mails with e-PHI encrypted? If not, are staff provid confidentiality statements about the risks of unencrypted emails?
Administrative Safeguards
Awareness
Has the office designated an individual to oversee HIPAA training?
Has the office conducted a HIPAA risk assessment previously?
Has the entire Health Care business function had HIPAA training?
Has every member gone through an annual HIPAA training ?
Has every member of the office reviewed and executed a confidentiality agreement?
Reporting of Incidents
Is there a policy or procedure for reporting potential office privacy or security incidents?
Has the office received training on the recognition of potential privacy or security incidents?
Vendor Contracts and Agreements
Does the office use any outside vendors to provide any medical or support services to the office?
If so, is there a written contract/agreement in place with these outside vendors?
Do these contracts/agreements expressly address HIPAA privacy and security rule issues?

Appendix - 3 - OHSE - HIRA Guide

Likelihood (Probability)		
Rare		The event may occur only in exceptional circumstances
Unlikely		The event may occur at sometime, say once in 10 years
Possible		The event should occur at sometime, say once in 3 years
Likely		The event will probably occur in most circumstances, say
Almost Certa		The event is expected to occur in most circumstances

Consequence (Impact)		
Descriptor	Level	Definition
Insignificant	Level 1	No Injury
Minor	Level 2	Injury/ill health requiring first aid
Moderate	Level 3	Injury/ill health requiring medical attention
Major	Level 4	Injury/ill health requiring hospital admission
Severe	Level 5	Fatality

Risk Matrix					
Likelihood	Consequence				
	Insignificant	Minor	M		Se
Almost Certa		HIGH	EX	EX	EXT
Likely	MEDIUM	HIGH		EX	EXT
Possible		MEDIUM		EX	EXT
Unlikely			M		EXT
Rare			M		H