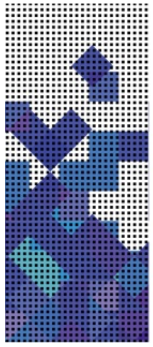

Sultanate of Oman
Information Technology Authority

e.oman

IT Risk Management Framework

GOVERNANCE & STANDARDS DIVISION

VALIDATION & DISTRIBUTION:

	Name	**Email**	**Issue date**
Issued by	Governance & Standards Division	standards@ita.gov.om	2017
Verified by			
Approved by	Steering Committee		

Distribution List	
1.	ITA
2.	All concerned government agencies
3.	Online publishing

DOCUMENT REVISION HISTORY:

Version	**Date**	**Author**	**Remarks**
1.0	2017	Governance & Standards	Creation of document

Contents

1 INTRODUCTION

Information technology is widely recognized as the engine that enables the government to provide better services to its citizens, and facilitating greater productivity as a nation. Organizations in the public sector depend on technology-intensive information systems to successfully carry out their missions and business functions. Information systems are subject to serious threats that can have adverse effects on organizational operations (i.e., missions, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation by exploiting both known and unknown vulnerabilities to compromise the confidentiality, integrity, or availability of the information being processed, stored, or transmitted by those systems. Threats to information and information systems can include purposeful attacks, environmental disruptions, and human/machine errors and result in great harm to the national and economic security interests of the Sultanate of Oman. Therefore, it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk—that is, the risk associated with the operation and use of information systems that support the missions and business functions of their organizations.

Organizational risk can include many types of risk (e.g., program management risk, investment risk, budgetary risk, legal liability risk, safety risk, inventory risk, supply chain risk, and security risk). Security risk related to the operation and use of information systems is just one of many components of organizational risk that senior leaders/executives address as part of their ongoing risk management responsibilities. Effective risk management requires that organizations operate in highly complex, interconnected environments using state-of-the-art and legacy information systems—systems that organizations depend on to accomplish their missions and to conduct important business-related functions. Leaders must recognize that explicit, well-informed risk-based decisions are necessary in order to balance the benefits gained from the operation and use of these information systems with the risk of the same systems being vehicles through which purposeful attacks, environmental disruptions, or human errors cause mission or business failure. Managing information security risk, like risk management in general, is not an exact science. It brings together the best collective judgments of individuals and groups within organizations responsible for strategic planning, oversight, management, and day-to-day operations—providing both the necessary and sufficient risk response measures to adequately protect the missions and business functions of those organizations.

The role of information security in managing risk from the operation and use of information systems is also critical to the success of organizations in achieving their strategic goals and objectives. Historically, senior leaders/executives have had a very narrow view of information security either as a technical matter or in a stovepipe that was independent of organizational risk and the traditional management and life cycle processes. This extremely limited perspective often resulted in inadequate consideration of how information security risk, like other organizational risks, affects the likelihood of organizations successfully carrying out their missions and business functions. This publication places

information security into the broader organizational context of achieving mission/business success. The objective is to:

Ensure that senior leaders/executives recognize the importance of managing information security risk and establish appropriate governance structures for managing such risk;

- Ensure that the organization's risk management process is being effectively conducted across the three tiers of organization, mission/business processes, and information systems;
- Foster an organizational climate where information security risk is considered within the context of the design of mission/business processes, the definition of an overarching enterprise architecture, and system development life cycle processes; and
- Help individuals with responsibilities for information system implementation or operation better understand how information security risk associated with their systems translates into organization-wide risk that may ultimately affect the mission/business success.

1.1 PURPOSE

The purpose of this framework document is to provide guidance for conducting risk assessments of government organizations. Risk assessments are part of an overall risk management process—providing senior leaders/executives with the information needed to determine appropriate courses of action in response to identified risks. In particular, this document provides guidance for carrying out each of the steps in the *risk assessment process* (i.e., preparing for the assessment, conducting the assessment, communicating the results of the assessment, and maintaining the assessment) and how risk assessments and other organizational risk management processes complement and inform each other.

1.2 TARGET AUDIENCE

This publication is intended to serve a diverse group of risk management professionals including:

- Individuals with oversight responsibilities for risk management (e.g., heads of agencies, chief executive officers, chief operating officers, risk executive [function]);
- Individuals with responsibilities for conducting organizational missions/business functions (e.g., mission/business owners, information owners/stewards, authorizing officials);
- Individuals with responsibilities for acquiring information technology products, services, or information systems (e.g., acquisition officials, procurement officers, contracting officers);
- Individuals with information system/security design, development, and implementation responsibilities (e.g., program managers, enterprise architects, information security architects, information system/security engineers, information systems integrators);

- Individuals with information security oversight, management, and operational responsibilities (e.g., chief information officers, senior information security officers,[10] information security managers, information system owners, common control providers); and
- Individuals with information security/risk assessment and monitoring responsibilities (e.g., system evaluators, penetration testers, security control assessors, risk assessors, independent verifiers/validators, inspectors general, auditors).

2 RISK ASSESSMENT METHODOLOGY

Government entity should use risk assessment to determine the extent of the potential threat and the risk associated with an Information Asset. The output of this process helps to identify appropriate controls for reducing or eliminating risk during the risk mitigation process.

Risk assessment exercise must be revisited at least annually (or whenever any significant change occurs in the organization) by Information Security Manager/Officer and all the new identified threats and vulnerabilities should be taken into consideration for the treatment. Previously identified (existing) risks should also be revisited to see if the controls applied are sufficient or need further treatment.

2.1 ASSET IDENTIFICATION

This document propose qualitative risk analysis model for assessing and maintaining the risk framework. The risk management team should comprise of individuals from various groups within the organization. Representatives from these groups should work together and identify the assets within their team that forms the information asset list. This list identifies the various assets as well as the category to which these assets belong as well as the location of the asset.

Asset Inventory exists in different forms and those that hold this information are known as information assets owners. This can be:

- Information / Data asset
- Technology Asset
- People Asset
- Service Asset

All the information assets of the organization should be identified and documented. Once identified, assets are labelled according to the pre-defined labelling criteria (Information Labelling and Handling Procedure should be established by the organization).

Every information asset should have an asset owner or/and an asset custodian. Owner and Custodian of each asset are maintained at respective asset inventories. From risk management perspective, the asset owner will be considered as the risk owner, and will be responsible to take appropriate actions and adopt effective controls to lower the risk.

2.2 THREAT IDENTIFICATION

A threat is the potential for a particular threat-source to successfully exercise (accidentally trigger or intentionally exploit) a particular vulnerability. A Threat-Source is either; (1) intent and method targeted at the intentional exploitation of a vulnerability or (2) a situation and method that may accidentally trigger a vulnerability. A vulnerability is a weakness that can be accidentally triggered or intentionally exploited.

A threat-source does not present a risk when there is no vulnerability that can be exploited. In determining the likelihood of a threat, one must consider threat-sources, potential vulnerabilities, and existing controls.

2.2.1 2.1 Threat-Source Identification

The goal of this step is to identify the potential threat-sources and compile a threat statement listing potential threat-sources that are applicable to the Information Asset being considered.

A threat-source is defined as any circumstance or event with the potential to cause harm to an Information Asset. The common threat-sources can be natural, human, or environmental. In assessing threat-sources, it is important to consider all potential threat-sources that could cause harm to an Information Asset. For example, although the threat statement for an IT system located in a desert may not include “natural flood” because of the low likelihood of such an event’s occurring, environmental threats such as a bursting pipe can quickly flood a computer room and cause damage to an organization’s IT assets and resources. Humans can be threat-sources through intentional acts, such as deliberate attacks by malicious persons or disgruntled employees, or unintentional acts, such as negligence and errors.

A deliberate attack can be either (1) a malicious attempt to gain unauthorized access to an IT system (e.g., via password guessing) in order to compromise system and data integrity, availability, or confidentiality or (2) a benign, but nonetheless purposeful, attempt to circumvent system security. One example of the latter type of deliberate attack is a programmer's writing a Trojan horse program to bypass system security in order to "get the job done."

Common Threat-Sources:

- **Natural Threats**—Floods, earthquakes, tornadoes, landslides, avalanches, electrical storms, and other such events.
- **Human Threats**—Events that are either enabled by or caused by human beings, such as unintentional acts (inadvertent data entry) or deliberate actions (network based attacks, malicious software upload, unauthorized access to confidential information).
- **Environmental Threats**—Long-term power failure, pollution, chemicals, liquid leakage.

2.2.2 2.2 Motivation and Threat Actions

Motivation and the resources for carrying out an attack make humans potentially dangerous threat-sources. Table 3-1 presents an overview of many of today's common human threats, their possible motivations, and the methods or threat actions by which they might carry out an attack.

This information will be useful to organizations studying their human threat environments and customizing their human threat statements. In addition, reviews of the history of system breakins; security violation reports; incident reports; and interviews with the system administrators, help desk personnel, and user community during information gathering will help identify human threat-sources that have the potential to harm an IT system and its data and that may be a concern where a vulnerability exists.

Table 1 – Threat source and their motivations.

Threat-Source	Motivation	Threat Actions
Hacker, cracker	Challenge Ego Rebellion	• Hacking • Social engineering • System intrusion, break-ins • Unauthorized system access
Computer criminal	Destruction of information Illegal information disclosure Monetary gain Unauthorized data alteration	• Computer crime (e.g., cyber stalking) • Fraudulent act (e.g., replay, impersonation, interception) • Information bribery • Spoofing • System intrusion
Terrorist	Blackmail Destruction Exploitation Revenge	• Bomb/Terrorism • Information warfare • System attack (e.g., distributed denial of service) • System penetration • System tampering
Industrial espionage (companies, foreign governments, other government interests)	Competitive advantage Economic espionage	• Economic exploitation • Information theft • Intrusion on personal privacy • Social engineering • System penetration • Unauthorized system access (access to classified, proprietary, and/or technology-related information)
Insiders (poorly trained, disgruntled, malicious, negligent, dishonest, or terminated employees)	Curiosity Ego Intelligence Monetary gain Revenge Unintentional errors and omissions (e.g., data entry error, programming error)	• Assault on an employee • Blackmail • Browsing of proprietary information • Computer abuse • Fraud and theft • Information bribery • Input of falsified, corrupted data • Interception • Malicious code (e.g., virus, logic

		bomb, Trojan horse) • Sale of personal information • System bugs • System intrusion • System sabotage • Unauthorized system access

An estimate of the motivation, resources, and capabilities that may be required to carry out a successful attack should be developed after the potential threat-sources have been identified, in order to determine the likelihood of a threat's exercising a system vulnerability.

The threat statement, or the list of potential threat-sources, should be tailored to the individual organization and its processing environment (e.g., end-user computing habits). In general, information on natural threats (e.g., floods, earthquakes, storms) should be readily available.

Output: ***A threat statement containing a list of threat-sources that could exploit system vulnerabilities***

2.3 VULNERABILITY IDENTIFICATION

Vulnerability: A flaw or weakness in system security procedures, design, implementation, or internal controls that could be exercised (accidentally triggered or intentionally exploited) and result in a security breach or a violation of the system's security policy.

The analysis of the threat to an Information Asset must include an analysis of the vulnerabilities associated with the system environment. The goal of this step is to develop a list of system vulnerabilities (flaws or weaknesses) that could be exploited by the potential threat-sources.

Table 2 – Vulnerabilities and Threats.

Vulnerability	Threat-Source	Threat Action
Terminated employees' system identifiers (ID) are not removed from the system	Terminated employees	Dialing into the company's network and accessing company proprietary data
Company firewall allows inbound telnet, and *guest* ID is enabled on XYZ server	Unauthorized users (e.g., hackers, terminated employees, computer criminals, terrorists)	Using telnet to XYZ server and browsing system files with the *guest* ID
The vendor has identified flaws in the security design of the system; however, new patches have not been applied to the system	Unauthorized users (e.g., hackers, disgruntled employees, computer criminals, terrorists)	Obtaining unauthorized access to sensitive system files based on known system vulnerabilities
Data center uses water sprinklers to suppress fire; tarpaulins to protect hardware and equipment from water damage are not in place	Fire, negligent persons	Water sprinklers being turned on in the data center

Output: A list of the system vulnerabilities (observations) that could be exercised by the potential threat-sources

2.4 Control Analysis

The goal of this step is to analyze the controls that have been implemented, or are planned for implementation, by the organization to minimize or eliminate the likelihood (or probability) of a threat's exercising a system vulnerability.

To derive an overall likelihood rating that indicates the probability that a potential vulnerability may be exercised within the construct of the associated threat environment, the implementation of current or planned controls must be considered. For example, a vulnerability (e.g., system or procedural weakness) is not likely to be exercised or the

likelihood is low if there is a low level of threat-source interest or capability or if there are effective security controls that can eliminate, or reduce the magnitude of, harm.

Sections 4.1 and 4.2 below, respectively, discuss control methods, and control categories.

2.4.1 4.1 Control Methods

Security controls encompass the use of technical and nontechnical methods. Technical controls are safeguards that are incorporated into computer hardware, software, or firmware (e.g., access control mechanisms, identification and authentication mechanisms, encryption methods, intrusion detection software). Nontechnical controls are management and operational controls, such as security policies; operational procedures; and personnel, physical, and environmental security.

2.4.2 4.2 Control Categories

The control categories for both technical and nontechnical control methods can be further classified as either preventive or detective. These two subcategories are explained as follows:

- **Preventive controls** inhibit attempts to violate security policy and include such controls as access control enforcement, encryption, and authentication.
- **Detective controls** warn of violations or attempted violations of security policy and include such controls as audit trails, intrusion detection methods, and checksums.

The implementation of such controls during the risk mitigation process is the direct result of the identification of deficiencies in current or planned controls during the risk assessment process
(e.g., controls are not in place or controls are not properly implemented).

Output: List of current or planned controls used for the IT system to mitigate the likelihood of a vulnerability's being exercised and reduce the impact of such an adverse event

2.5 RISK ASSESSMENT

The adverse impact of a security event can be described in terms of loss or degradation of any, or a combination of any, of the following three security goals: integrity, availability, and confidentiality. The following list provides a brief description of each security goal and the consequence (or impact) of its not being met:

- **Loss of Integrity.** System and data integrity refers to the requirement that information be protected from improper modification. Integrity is lost if unauthorized changes are made to the data or IT system by either intentional or accidental acts. If the loss of system or data integrity is not corrected, continued use of the contaminated system or corrupted data could result in inaccuracy, fraud, or erroneous decisions. Also, violation of integrity may be the first step in a successful attack against system availability or confidentiality. For all these reasons, loss of integrity reduces the assurance of an IT system.

- **Loss of Availability.** If a mission-critical IT system is unavailable to its end users, the organization's mission may be affected. Loss of system functionality and operational effectiveness, for example, may result in loss of productive time, thus impeding the end users' performance of their functions in supporting the organization's mission.

- **Loss of Confidentiality.** System and data confidentiality refers to the protection of information from unauthorized disclosure. The impact of unauthorized disclosure of confidential information can range from the jeopardizing of national security to the disclosure of Privacy Act data. Unauthorized, unanticipated, or unintentional disclosure could result in loss of public confidence, embarrassment, or legal action against the organization.

Risks to information assets are assessed for breach of Confidentiality, Integrity, and Availability first, and then the combined risk is calculated using the formula defined in this section below.

Confidentiality Risk = Impact of Confidentiality % * Probability of Confidentiality %
Availability Risk = Impact of Availability % * Probability of Availability %
Integrity Risk = Impact of Integrity % * Probability of Integrity %

2.5.1 Probability Determination

To derive probability rating that a potential vulnerability may be exercised within the construct of the associated threat environment, the following governing factors must be considered:

- Threat-source motivation and capability
- Nature of the vulnerability
- Existence and effectiveness of current controls.

The probability that a potential vulnerability could be exercised by a given threat-source can be described as very high, high, medium, low, or very low. Table below describes these five levels.

Table 3 - Probability of Occurrence (breach of C, I, A)

Rating	Description	Probability of Occurrence
1	Rare	Highly unlikely, but it may occur in exceptional circumstances. It could happen, but probably never will.
2	Unlikely	Not expected, but there's a slight possibility it may occur at some time.
3	Possible	The event might occur at some time as there is a history of casual occurrence at the similar institutions.
4	Likely	There is a strong possibility the event will occur as there is a history of frequent occurrence at similar institutions.
5	Almost Certain	Very likely. The event is expected to occur in most circumstances as there is a history of regular occurrence at similar institutions.

2.5.2 Impact Determination

The adverse impact of the loss of confidentiality, integrity, and availability of the information asset, resulting from exploitation of a vulnerability by a threat, is determined based on the sensitivity of the information asset and the level of protection required. The information asset owners are the ones responsible for determining the impact level for their information assets.

The table below provides description of impact at the scale of 1 to 5 (with appropriate ratings), and is described from five different perspectives (Financial Impact, Client & Staff health & Safety, Business interruption, Reputation & Image, and Corporate Objectives).

Table 4 - Impact of breach of C, I, A

Rating	Description	Financial Impact	Clients & Staff Health & Safety	Business Interruption	Reputation & Image	Corporate Objectives
1	Insignificant	Minimal financial loss; Less than $300,000	No or only minor personal injury; First Aid needed but no days lost	Negligible; Critical systems unavailable for less than one hour	Negligible impact	Resolved in day-to-day management
2	Minor	$300,000 to $2M; not covered by insurance	Minor injury; Medical treatment & some days lost	Inconvenient; Critical systems unavailable for several hours	Adverse local media coverage only	Minor impact
3	Moderate	$2M to $5M; not covered	Injury; Possible hospitalization	Client dissatisfaction; Critical systems	Adverse capital city	Significant impact

		by insurance	& numerous days lost	unavailable for less than 1 day	media coverage	
4	Major	$5M to $10M; not covered by insurance	Single death &/or long-term illness or multiple serious injuries	Critical systems unavailable for 1 day or a series of prolonged outages	Adverse and extended national media coverage	Major impact
5	Catastrophic	Above $10M; not covered by insurance	Fatality(ies) or permanent disability or ill-health	Critical systems unavailable for more than a day (at a crucial time)	Demand for government inquiry	Disastrous impact

Note: Agencies must update the financial impact range in the table above considering their risk appetite and financial authority manual.

Thus the risk Score (for C, I, and A) may be between 1 (minimum value) and 5 (maximum value).

Business Impact = 1 to 5

Likelihood = 1 to 5

It is important to calculate the risk Score as it help in prioritizing the treatment of risk. If we do a risk treatment on assets that has a low risk score, the cost to mitigate risk on those assets might be much higher than the loss it could cause to the business.

Table 5 – Risk Impact Matrix

		Impact				
		1	2	3	4	5
Likelihood	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	20	25

Table 6 – Risk Impact Definitions

Qualitative Values	Semi-Quantitative Values	Description
Very High	21-25	**Very high** risk means that a threat event could be expected to have **multiple severe or catastrophic** adverse effects on organizational operations, organizational assets, individuals, other organizations, or the Nation.
High	16-20	**High risk** means that a threat event could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Moderate	10-15	**Moderate risk** means that a threat event could be expected to have a **serious** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Low	6-9	**Low risk** means that a threat event could be expected to have a **limited** adverse effect on organizational operations, organizational assets, individuals, other organizations, or the Nation.
Very Low	1-5	**Very low** risk means that a threat event could be expected to have a **negligible** adverse effect on organizational operations,

		organizational assets, individuals, other organizations, or the Nation.

2.5.3 Combined Risk Score

The Combined Risk (CR) is not a general average based on Confidentiality (C), Integrity (I) and Availability (A) values, but rather a weighted average where all other conditions from the impact assessment are taken into account.

When you need to find a value for the combined risk, one would typically choose between:

1. Average
2. Worst case

However, in cases where only one value differs greatly from the other, the average will hide the deviated value, and worst case will become very high. We have therefore chosen to use both average and worst case.

Use the following formula to calculate the CR.

Combined Risk = (Average + Worst Case) / 2

Where;

Average = (Confidentiality Risk + Integrity Risk + Availability Risk) / 3

Worst Case = Highest Risk value among Confidentiality Risk, Integrity Risk, and Availability Risk

2.6 Risk Acceptance Criteria

The [GOVERNMENT ENTITY]'s management accepts risk with a value of 9 (nine) or less as per the [GOVERNMENT ENTITY]'s risk management framework. Any risk value above 9 (nine) would have to be taken up as a deviation and [GOVERNMENT ENTITY]'s management should accept the risk as a deviation or take further steps to ensure the risk value is kept within the threshold.

Table 7 – Risk Acceptance Range

Risk Category	Risk Range
Very Low	1 to 5
Low	6 to 9
Medium	10 – 15
High	16 to 20
Very High	21 to 25

3 RISK TREATMENT

The risk treatment plan is arrived on the basis of the risk analysis done. The risk analysis will provide pointers on the areas of improvement. The treatment plan will be identified and documented as part of the risk assessment matrix. This will give a complete picture of the full life cycle of risk assessment and mitigation. This will be covered under the column “risk mitigation” under the risk assessment matrix.

3.1 METHODS OF HANDLING RISKS

3.1.1 Risk Mitigation

To limit the risk by implementing controls that minimizes the adverse impact of a threat's on an asset. By implementing anti-virus server in the organization does not ensure that the assets will be protected from virus attacks. This is a method of minimizing the risk from known virus attacks. So by implementation of anti-virus and keeping virus definitions updated, we are limiting the risk of virus attack. Also by taking backup at regular frequency, we are limiting the effect of the threat if it materializes.

3.1.2 Risk Transfer

To transfer the risk by using other options to compensate for the loss, such as purchasing insurance. Risk can also be transferred by outsourcing (having a contract with third party vendors). In the means of maintenance contract (MC's) or any other agreement of having spares at our location.

3.1.3 Risk Avoidance

To avoid the risk by eliminating the risk cause and / or consequence. If there is an old system (Windows 98 running some legacy/proprietary application), which cannot be patched for the current vulnerabilities, can be taken off the network to avoid risk of being compromised.

3.1.4 Risk Acceptance

It might not always be possible or financially feasible to reduce risks to an acceptable level. In these circumstances, it might be necessary to knowingly and objectively accept the risk.

For example: Due to some testing purpose we might need to move one of the servers to the DMZ for a particular period of time. Since this testing is mandatory, it can be

considered as an acceptable risk for that period. But this has to be agreed by the management and the asset owners.

or to implement controls to lower the risk to an acceptable level. We need to give a high priority to the business requirements, while also looking at how to safeguard information. There are instances where we require accepting certain risk and seeing to that the business requirements are met.

3.1.5 Residual Risk

After the risk treatment decisions have been implemented, there will always be risks with values higher than the acceptable threshold – these risks are called residual risk. The residual risks are presented to the management committee for acceptance and management agrees to accept the residual risks. The accepted residual risks are documented and approved by management.

All the residual risks will be re-visited every time risk assessment is being revised or a new threat is discovered.

4 APPENDIX A – LIST OF THREATS & VULNERABILITIES

One of the initial planning steps in a risk management program is to generate a comprehensive list of sources of threats, risks, and events that might have an impact on the ability of the organization to achieve its objectives as identified in the definition of scope and the framework. These events might prevent, degrade, delay or enhance the achievement of those objectives.

In general, a risk can be related to or characterized by:

- It's origin—e.g., threat agents such as hostile employees, employees not properly trained, competitors, governments, etc.
- A certain activity, event or incident (i.e., threat)—e.g., unauthorized dissemination of confidential data, competitor deployment of a new marketing policy, new or revised data protection regulations, an extensive power failure
- Its consequences, results or impact—e.g., service unavailability, loss or increase of market share/profits, increase in regulation, increase or decrease in competitiveness, penalties, etc.
- A specific reason for its occurrence—e.g., system design error, human intervention, prediction or failure to predict competitor activity
- Protective mechanisms and controls (together with their possible lack of effectiveness)—e.g., access control and detection systems, policies, security training, market research and surveillance of market
- Time and place of occurrence—e.g., a flood in the computer room during extreme environmental conditions

4.1 THREATS

- Access to the network by unauthorized persons
- Bomb attack
- Bomb threat
- Breach of contractual relations
- Breach of legislation
- Compromising confidential information
- Concealing user identity
- Damage caused by a third party
- Damages resulting from penetration testing
- Destruction of records
- Disaster (human caused)
- Disaster (natural)
- Disclosure of information
- Disclosure of passwords
- Eavesdropping
- Embezzlement
- Errors in maintenance
- Failure of communication links
- Falsification of records
- Fire
- Flood
- Fraud
- Industrial espionage
- Information leakage
- Interruption of business processes
- Loss of electricity
- Loss of support services
- Malfunction of equipment
- Malicious code
- Misuse of information systems
- Misuse of audit tools
- Pollution
- Social engineering
- Software errors
- Strike
- Terrorist attacks
- Theft
- Thunderstroke
- Unintentional change of data in an information system
- Unauthorized access to the information system
- Unauthorized changes of records
- Unauthorized installation of software
- Unauthorized physical access
- Unauthorized use of copyright material
- Unauthorized use of software
- User error
- Vandalism

4.2 VULNERABILITIES

- Default passwords not changed
- Disposal of storage media without deleting data
- Equipment sensitivity to moisture and contaminants
- Equipment sensitivity to temperature
- Inadequate cabling security
- Inadequate capacity management
- Inadequate change management
- Inadequate classification of information
- Inadequate control of physical access
- Inadequate maintenance
- Inadequate network management
- Inadequate or irregular backup
- Inadequate password management
- Inadequate physical protection
- Inadequate protection of cryptographic keys
- Inadequate replacement of older equipment
- Inadequate security awareness
- Inadequate segregation of duties
- Inadequate segregation of operational and testing facilities
- Inadequate supervision of employees
- Inadequate supervision of vendors
- Inadequate training of employees
- Incomplete specification for software development
- Insufficient software testing
- Lack of access control policy
- Lack of clean desk and clear screen policy
- Lack of control over the input and output data
- Lack of internal documentation
- Lack of or poor implementation of internal audit
- Lack of policy for the use of cryptography
- Lack of procedure for removing access rights upon termination of employment
- Lack of protection for mobile equipment
- Lack of redundancy
- Lack of systems for identification and authentication
- Lack of validation of the processed data
- Location vulnerable to flooding
- Poor selection of test data
- Uncontrolled download from the Internet
- Uncontrolled use of information systems
- Unmotivated employees
- Unprotected public network connections
- User rights are not reviewed regularly