Risk Assessment Report

Table of Contents

Executive Summary

The risk assessment team identified in this report, coordinated by the Information Security Officer, worked during the period from December 1, 2021 to December 16, 2021 to analyze and assess the risks that threaten the information systems infrastructure of X, which is owned by X and managed by the Information Technology Department. The results of the overall classification of the system as an important system for the functioning of X were. The information technology infrastructure system in the company is designed to contain an effective system to avoid the complete breakdown of the infrastructure. It also contains a set of security, protection, support and alternative systems to be activated in case of need. In addition, the system is characterized by the fact that there is not a single part of the infrastructure that causes the breakdown of all systems, and that each part is specialized in a specific field and has practical alternatives in the event of its failure. The information technology infrastructure supports the provision of documents and information on the progress of operations and the provision of X services to employees and customers, and these documents are available in another form in cases of need by employees, and therefore the data and information contained in the system are necessary for the workflow of the company and the performance of its services, but its unlikely disruption will not lead to Completely disrupting the work of the company, the provision of its services, and the decision-making process in it.

This report contains the detailed results of the process of assessing the risks and weaknesses that threaten the system and the results of studying the control requirements necessary to protect the system, as well as an action plan to implement these controls from defining responsibilities and the schedule for implementing the plan, which was determined until mid-December 2021. The purpose and objective of the risk assessment and analysis report is to:

- Identifying and evaluating the threats faced by the information system.
- Determining the necessary controls and procedures to protect the information system from such threats.
- Provide appropriate justifications for the material cost necessary to implement the controls and procedures for the security and protection of the information system.
- Helping decision makers in X to understand the consequences of information system security breaches and their impact on the workflow and company interests.
- Create an action plan to respond to the risks that threaten the information system in the X and work to avoid those risks or reduce their effects.

The scope of the risk assessment report includes the information systems infrastructure system of X, which is located in X at its headquarters in the State of Libya, and includes all parts

and components of the system, hardware, software, work procedures and information security controls currently applied to the system.

Through various risk assessment approaches, **qualitative** assessment has been adopted in this RAR of the system. The Risk Assessment identifies the current level of risk to appropriately determine the values for risks (e.g., very low, low, moderate, high, very high) and provides risk mitigation recommendations for management review. The information systems infrastructure supports the working mechanisms of all information and communication systems in X and the mechanisms for exchanging data and data between those systems. Therefore, the greatest focus will be on the third level, which includes all information and communication systems in X, its location(s), security classification and borders to meet the security objectives.

Information Systems	Location(s)	Confidentiality	Integrity	Availability		Overall Risk Level
Libyana Web Server	Headquarters Tripoli, Libyana Server Room	H	H	M	Software application, customer, records, financial services	H
MySQL Server	Headquarters Tripoli, Libyana Data Center	H	M	H	Personal identifiable information, metadata, Employee-related information, Customer-related information	H
Libyana Email Server	Headquarters Tripoli, Libyana Server Room	VH	H	M	SMTP, email addresses, email content	H
Libyana Firewall	Headquarters Tripoli, Between Libyana internal network and the internet	H	M	L	Security policies, transmitted sensitive information	M
Libyana Windows Server	Headquarters Tripoli, Libyana Server Room	VH	H	VH	User accounts, DHCP, DNS, and Active Directory	VH
Libyana Computer Systems	Headquarters Tripoli, and Branch Benghazi	H	H	H	Downloaded applications	H

VH Very High H High M Moderate L Low VL Very Low

Fig.1. Scope risk assessment across Tier 3

The risk assessment identified 20 risks in all of X's critical information security components and the overall level of risk was High. In this report, Appendix B contains the Acceptable Use Policy which is a method that can be followed to mitigate these risks. By implementing these policies, X can conserve and use information technology resources safely in its business operations. The following information categorizes the number of risks identified in X with their respective levels:

- 1 risk were rated "**Low**".
- 4 risks were rated "**Moderate**".
- 4 risks were identified were rated "**Very High**"
- 11 risks were rated "**High**".

Purpose

The purpose of this Risk Assessment Report (RAR) is to provide the operating administration management at the company X, with an assessment of the management, operational and technical security controls that are currently in place to secure the company's operational system (Williams, 2018). This risk assessment also aims at analyzing the risks inherent with the application of the company's security system, which serves to protect the system used for handling business operations and support the confidentiality of the different departments in the company. The report will establish a baseline assessment of risks in order to identify the possible threats, based on the system's vulnerabilities and their impact on the organization's operations.

Through various risk assessment approaches, qualitative assessment has been adopted in this RAR of the system. The Risk Assessment identifies the current level of risk to appropriately determine the values for risks (e.g., very low, low, moderate, high, very high) and provides risk mitigation recommendations for management review. Because Risk assessments are often not precise instruments of measurement, this RAR will not eliminate the risk, however, it can be minimized by the application of IT security controls. In addition, RA reflects the limitations of the techniques employed, tools, and specific assessment methodologies.

Assumptions and Constraints

Different aspects of the organization's operational activities and system are to be considered during this risk assessment report, therefore different assumptions and constraints are to be adopted for risk assessment. Firstly, in terms of threat sources, identifying the appropriate sources of threat will help the organization both in the current risk assessment and in future reports, where several steps will not need to be repeated during every new assessment (Stoneburner, Feringa and Goguen, 2002). The threat sources to be considered in this assessment mainly include adversarial sources which cover a wide group of possible threats. Due to the fact that the primary information system at X seeks great confidentiality, where each employee must only be exposed to information to do with their specific department, adversarial threats are of great significance and could pose great danger to the company's security. Although the adversarial threats are the most significant to the nature of X's operations, and are considered to pose the greatest risks, other threats are also valid and may include accidental threats, structural threats and environmental threats.

Different threat events must also be considered during the risk assessment as they are directly related to the threat source. For X, threat events may be divided into adversarial and non-adversarial, where both types cover several scenarios that may occur. For adversarial events, threats include the creation of attack tools (phishing attacks, counterfeit certificates, injecting

malicious components into the supply chain); exploiting unauthorized access and information into the system, obtaining sensitive information and modifying existing information. On the other hand, non-adversarial events include incorrect privilege systems, which is a significant point in X company, where it aims to limit the access of information by different departments. Other events are fire or flood at the facility, system error, malfunctions in the system's software products and poor performance and communication.

The assumptions used in this risk assessment based on organizational direction and assessment team expertise in X include the following:

- Continuous monitoring of the components of the mission / business department and risks at the organizational level.
- The common controls implemented by X in meeting the specific requirements.
- With regard to network, system, application, communication, and contract for IT services, this assessment should assume and take into account some of the following characteristics such as technical, environmental and operational related to X's information system.
- X will be assumed that it is using the VPN for secure remote connection.
- Implementation and configuration of firewalls in X networks instead of using IDS and IPS.

Assessment Approach

Through various risk assessment approaches, qualitative assessment has been adopted in this RAR of the system. The Risk Assessment identifies the current level of risk to appropriately determine the values for risks (e.g., very low, low, moderate, high, very high) and provides risk mitigation recommendations for management review. Because Risk assessments are often not precise instruments of measurement, this RAR will not eliminate the risk, however, it can be minimized by the application of IT security controls. In addition, RA reflects the limitations of the techniques employed, tools, and specific assessment methodologies.

Time Frame

The effectiveness time frame of the risk assessment gives the company an idea of how long the risk assessment is valid for before it must be conducted once again (Fikri, Putra, Suryanto and Ramli, 2019). In the case of this report, it is to provide a comprehensive assessment of the different Tiers of the organization while giving special attention to the security of the information system technologies. Therefore, this risk assessment is expected to remain valid as a source of decision support for 18 months, unless new risk assessments will be required in the case of introducing new technologies or security controls to the system or launching new editions and updates to the already existing system used at X.

Questionnaire

These some of the key questions and their respective answers that have asked to the stakeholders in X to have a better understand the organization. Appendix A contain a full Questionnaire that has be used through this risk assessment.

I. What is access control in a pharmaceuticals and medical equipment company?

- Hospital access control systems are unique in comparison to other forms of access control. To protect both patients and staff, they must be able to restrict access to sensitive areas, prevent the spread of illness, track and prevent the theft of key healthcare equipment and drugs, and protect both patients and staff.

II. How does the organization now manage risk?

- Doing control activities decreases or eliminates X's danger. Assuring a possible impact of a risk or outsourcing risk-related operations to another business are two ways X transfer risk.

III. Is there a risk assessment mechanism in place in the company and how is it expected to help?

- X and its workers must be protected while also adhering to the law by doing a risk assessment. Using this tool helps you identify and prioritize the hazards that are most likely to cause damage in your workplace.

IV. In the future, the company's business focus will change substantially due to risk assessment?

- Risk management helps X identify and handle the risks your organization faces, improving the likelihood that your business objectives will be met. Taking a systematic approach to identifying and mitigating the threats to your company's operations is the essence of risk management.

Risk Model

for Libyana RA

The risk model defines the risk factors that are assessed and the relationships between them. The risk factors are:

1. Threat Sources
2. Threat Events
3. Vulnerabilities
4. Adverse Impacts and Likelihood

These risk factors determine the risk levels within Libyana organization.

Threat sources with adverse characteristics (Capability, Intent and Targeting) initiates threat events with a sequence of actions or scenarios. These threat events exploit the vulnerabilities that exist in Libyana causing adverse impacts. The adverse impacts with risk as a combination of impact and likelihood produce risks to organizational assets, operations, individuals, and other organization.

1 Threat Sources

Adversarial and Non-Adversarial Threats

Adversarial: Individual, Groups, Competitors - High Risk

Non-Adversarial: Accidental, Structural, and Natural - Medium to Low Risk

Initiate

2 Threat Events

> Creating phishing attacks
> Delivering malware and crime to internal organization information system.
> Access Of unauthorized staff to confidential information
> Obtain sensitive information due to lack Of encryption and secured system.

Exploit

3 Vulnerabilities

> poor encryption System
> Idle and guest accounts of previous employees not removed
> Passwords not set to expire
> Poor fire sprinkler system in data center
> Access privileges are not updated according to needs of departments
> Important and confidential data is Often stored on USB devices

Cause & produce

4 Adverse Impacts and Likelihood

The mentioned threats can have adverse impacts on the company's security and confidentiality where the adversarial threats are considered high risk due to the fact that the system has several vulnerable points. The of such threats occurring is therefore higher due to the mentioned vulnerabilities.

Risk Assessment Methodology:

The risk assessment methodology was selected according to the method attached to the special publication, A Guide to Conducting Risk Assessments, (SP) 800-30R1 issued by the National Institute of Standards and Technology (NIST). This methodology is one of the specialized methods for assessing the risks of information systems and determining the level of importance of the system to the workflow in X. In this risk assessment report, we will conduct the risk assessment by following these steps:

1. Prepare for assessment by identifying scope
2. Identify threat sources
3. Identify vulnerabilities and predisposing conditions
4. Determine likelihood
5. Determine impact
6. Determine risks and uncertainties
7. Detailed results
8. Monitor risk factors going forward

Risk Assessment Team and Participants

The work team that carried out the process of assessing risks and determining the necessary controls for information security and protection of the information system, and prepared and reviewed the final report, consisting of:

Name	Department	Job Description	The Role
Ahmed Zain	Information Technology Management	IT department manager	Consultant
Mohammed Mohamed	Information Technology Management	IT technician	Team Member
Eslam Tarrum	Information Technology Management	IT technician	Team Member

Data Sources

Additional data collection was conducted through the use of automated vulnerability scanners, manual inspection of the state of various controls (i.e., technical, process, operational, and management) and penetration testing (Pen Test) as appropriate. Threat information was collected from databases, data files, tapes, models, manuals, directories, publications, periodicals, and human resources. Databases are the most direct means for accessing large amounts of both quantitative and qualitative data quickly. Examples of techniques and methodologies used throughout this risk assessment are shown below:

Questionnaire

The assessment team prepared a questionnaire addressing key security-related issues, current implemented policies, and holistic overview of Libyana mission/business processes. This questionnaire helped the risk assessment team to identify risks related to Libyana's critical information assists (see Appendix A)

Interviews

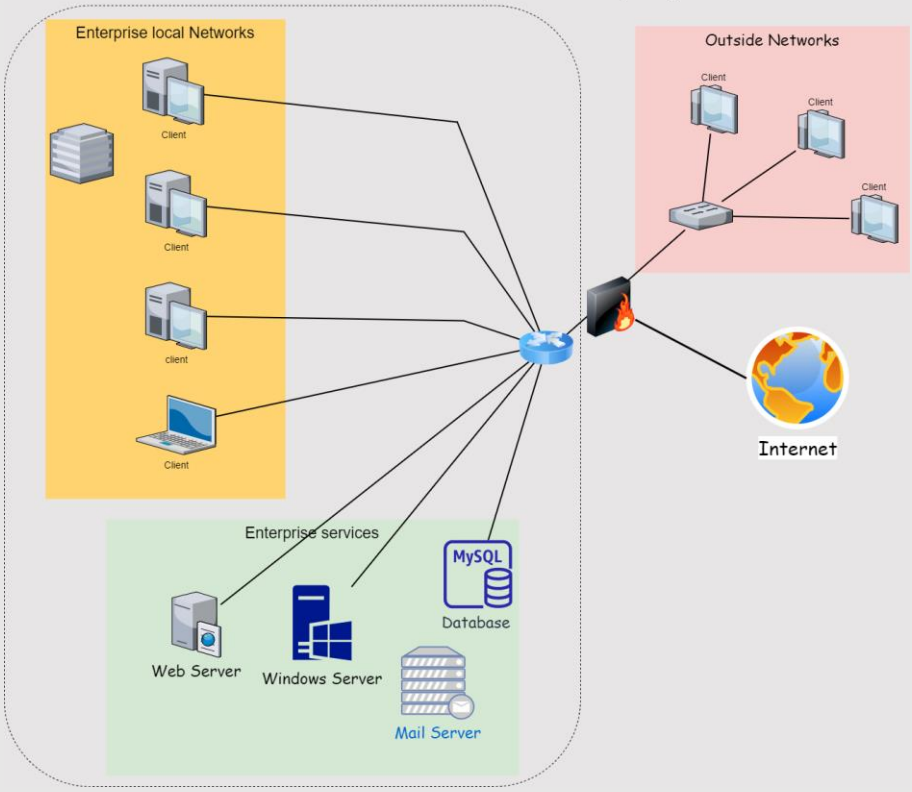
The risk assessment team conducted an interview with Libyana Chief Automation Technician to validate the questionnaire responses

Vulnerability Sources

The risk assessment team accessed identified vulnerabilities based on Common Sources Vulnerabilities and Exposures (CVE) databases

IT System Boundary Diagram

Figure: IT System Boundary Diagram



Technology Components

Technology Components	Description
Applications	Smartsheet Business Application
Server	Libyana Web Server Libyana Email Server Libyana Windows Server
Databases	MySQL Server
Operating Systems	Windows 10 Ubuntu 20.04
Networks	Libyana Firewall
Protocols	SMTP FTP SSL

Sensitivity

In this RAR, we used Federal Information Processing Standards 199 (FIPS) to provide security categorization of X information systems as shown in the figure below (See Appendix G). The general formula for expressing the security category for an information system is (where impact values can be low, moderate or high):

SC Information Type = {(**confidentiality**, impact), (**Integrity**, impact), (**Availability**, impact)}

Information Systems	Description	Confidentiality	Integrity	Availability
Libyana Web Server	Software application, customer, records, financial services	H	H	M
MySQL Server	Personal identifiable information, metadata, Employee-related information, Customer-related information	H	M	H
Libyana Email Server	SMTP, email addresses, email content	H	H	M
Libyana Firewall	Security policies, transmitted sensitive information	H	M	L
Libyana Windows Server	User accounts, DHCP, DNS, and Active Directory	H	H	H
Libyana Computer Systems	Downloaded applications	H	H	H

H High M Moderate L Low

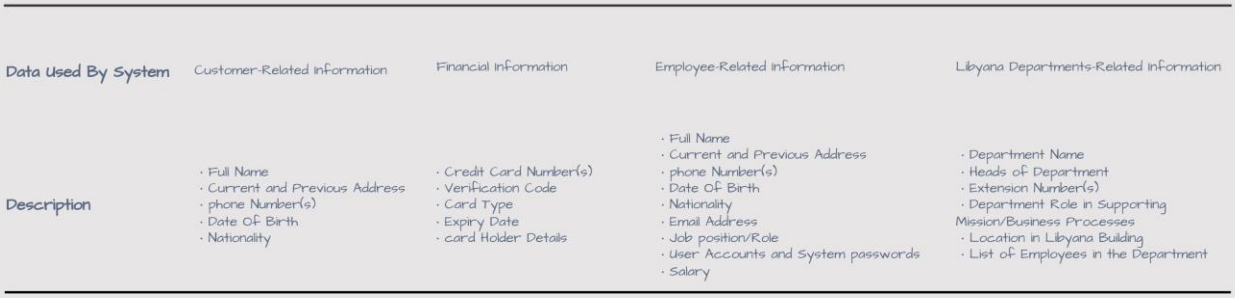
Physical Location(s)

This figure represents the physical locations of information system components:

Information Systems	Location(s)
Libyana Web Server	Headquarters Tripoli, Libyana Server Room
MySQL Server	Headquarters Tripoli, Libyana Data Center
Libyana Email Server	Headquarters Tripoli, Libyana Server Room
Libyana Firewall	Headquarters Tripoli, Between Libyana Internal network and the Internet
Libyana Windows Server	Headquarters Tripoli, Libyana Server Room
Libyana Computer Systems	Headquarters Tripoli, and Branch Benghazi

Data Used by System

This figure shows the Data categorization which used by the system besides a brief description for each category and what it contains:



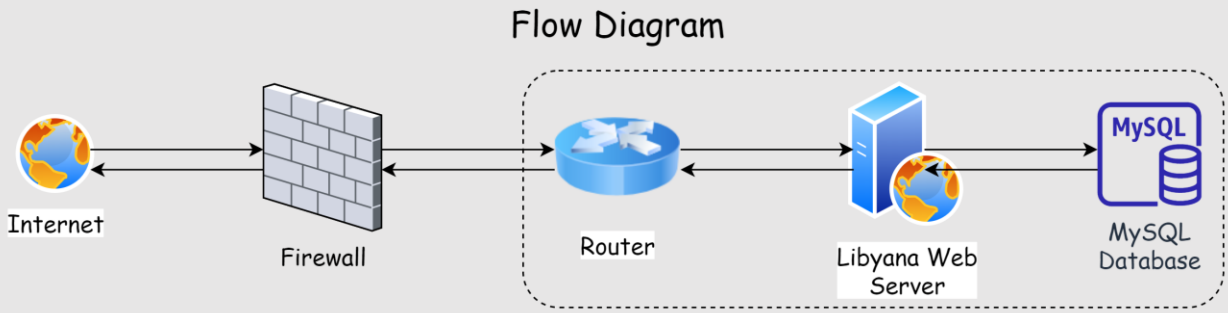
Users

This figure shows the users categorization in X information systems:

Users	Description
X Employees	The employees will be able o perform their daily X business processes and missions by having the access to the system through server rooms, computer systems, and data centers.
X Customer	Limited services such as tracking information and payment facilities will be provided to customers through accessing the system either by a mobile application or a web browser.
X Operations	Utilize information contained in the X database for management reporting. Generate reports and database queries.
X Security Team	Managing X information systems and maintain security configuration of the system at tier 3, and coordinating with level (Tier2) based on defined organizational risk frame at Tier 1.

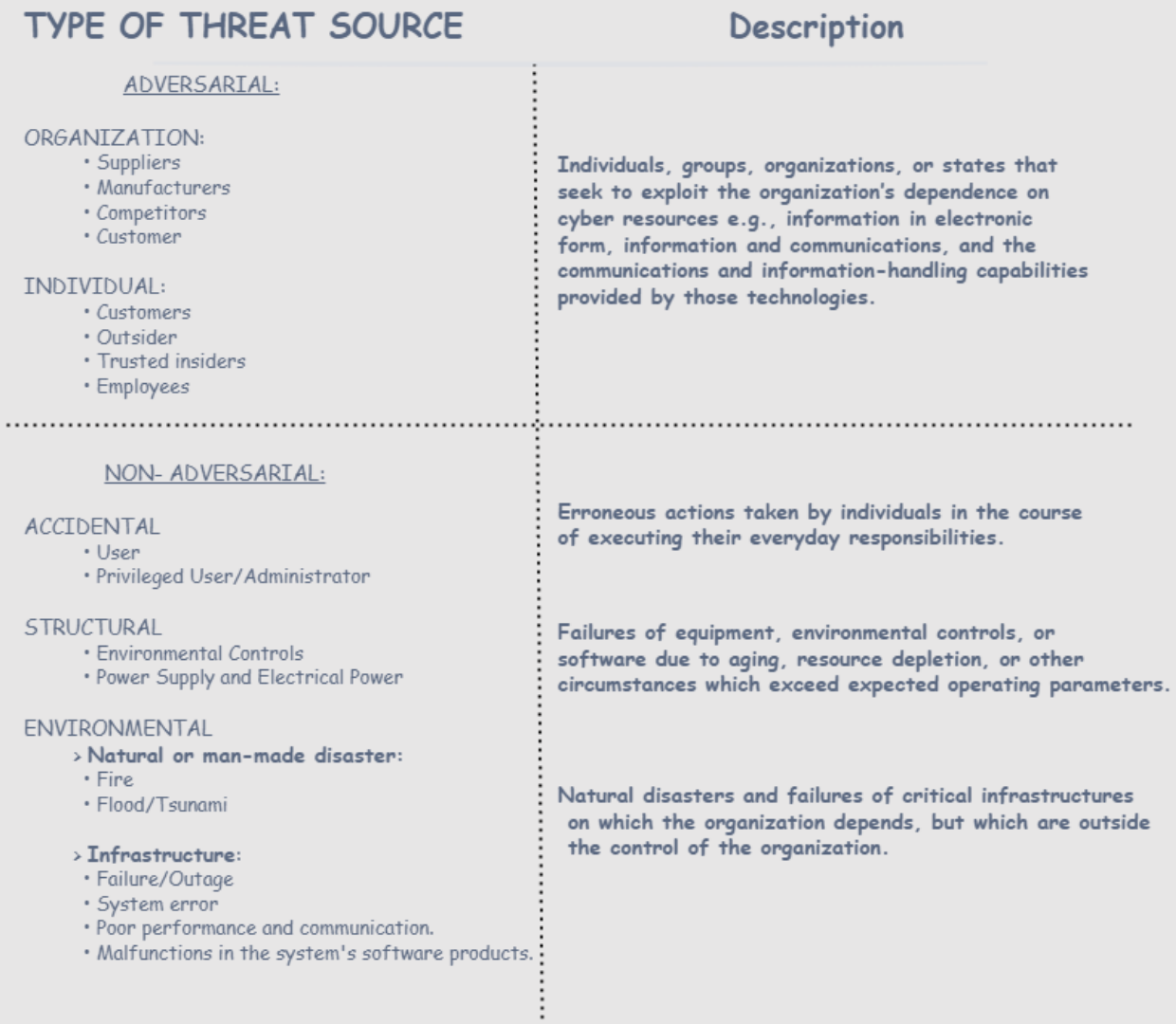
Flow Diagram

The flow diagram is representing the direction of information flow within X network which defines the scope of the risk assessment effort.



Threat Source

The main sources of threat to the company include, as mentioned, adversarial threats, where based on the company's operation, it seeks to keep each department confidential from other departments. In addition, the company deals with many suppliers, manufacturers and customers, therefore keeping its information system secure is top priority. In this case, individuals from both inside the company and outside may attempt to access unauthorized information, including competitors, and even trusted insiders who are the employees of the company. Unintentional acts can also represent threat sources where they can be indeliberate such as incorrect data entry and negligence. Furthermore, the non-adversarial sources can be environmental sources or natural threats such as long-term power failure, floods, earthquakes or fires which cannot be controlled by humans and pose danger to the system's security. Such threats however are of lower risk and are much less likely to happen compared to other adversarial threats and vulnerabilities. One of the significant vulnerabilities of a company such as X, is the access privileges where usernames and passwords must be set to expire in addition to enforcing regular password changes. This strengthens the system and makes unauthorized access more difficult. Such a vulnerability leads to a high risk of malicious use and computer crime effecting the company's confidentiality. Another vulnerability to the system is the existence of idle accounts belonging to previous employees or guests, in addition to the poor use of encryption within the system, thus making it easier for crime to occur. Malicious use and crime are one of the highest risks affecting the company, as the company possesses several vulnerabilities to encourage the risks of these threats. This table summarize threat sources and a brief description of each source.



Threat Identification

Threat identification is the process of identifying potential threat events that could be caused by threat sources identified for X as an organization. The identified threat sources are assessed based on its capability, intent and targeting. The identified threat events are classified based on various values of relevance to the organization and are characterized based on its tactics, techniques, and procedures. This table represents Threat Sources, Threat Event, Capability, Intent and Targeting.

Threat sources	Threat Event	Threat sources Characteristics		
		Capability	Intent	Targeting
Absence Of Two-Factor Authentication in Libyana payment mechanisms	Identify theft through user impersonation where attacker obtains sensitive resources such as credit card details of the impersonated user	Very High	High	High
Absence Of Server Room Security Policy	Conduct physical attacks on organizational facilities	High	High	Very High
Wet-pipe sprinkler system in Libyana Data Center	Fire would activate sprinkler system causing water damage & compromising the availability of Libyana	High	Very High	High
Spyware/malware authors use Of automated update setting for operating systems	Denial Of Service (DoS) attack through automatic updates. Effects resources available in induvial user accounts and operating systems	High	High	Very High
Spyware/malware authors use Of automated update setting for operating systems	Insert untargeted malware into downloadable software	Very High	High	High
Trusted employees using unsecure communication platforms for business sensitive information flow	Social Engineering techniques used by attackers to gain legitimate access to confidential and private information for the purpose of identity theft	Very High	High	High
Trusted employees using unsecure communication platforms for business sensitive information flow	Attacker delivering known malware to internal organizational information systems (e.g., virus via email).	High	High	Very High
Phishers taking advantage of the email platform that implement weak filters	Craft phishing attacks	Very High	High	High
Phishers taking advantage of the email platform that implement weak filters	Malware provided in the form of phishing emails to obtain private information such as login and password. Leads to unauthorized access to Libyana systems	High	High	High
Attacker / Weak permissions	Privilege Escalation	Very High	High	Very High

Threat sources	Threat Event	Threat sources Characteristics		
		Capability	Intent	Targeting
Absence of Server room Security policy (Insiders)	Data breach due to tampering and theft of confidential information stored in Libyana servers	High	Moderate	High
Absence of Server room Security policy (Insiders)	Compromise design. manufacture, and/or distribution of information system components (hardware)	High	Moderate	Moderate
The use of weak encryption techniques between users and Libyana application	Conduct communications interception attacks	High	Very High	High
The use of weak encryption techniques between users and Libyana application	Exposing data to risk of unauthorized disclosure	High	High	Very High
High privileged attackers accessing MySQL database	Exposing data to risk of unauthorized disclosure through privilege escalation. Executing unauthorized functions in the database	Very High	High	High
Attacking Libyana network because of absence of firewall	Network downtime performance due to spreading of viruses or malware	High	Moderate	Moderate
Hackers detect unsecure protocols	Attackers will be able to obtain all available communication through incoming and outgoing traffic within the network after reconnaissance process on the Libyana network.	High	High	Very High
Third party attempting to access the organization's data center	Exploiting unauthorized access and information into the system, obtaining sensitive information and modifying existing information.	Very High	High	High
Dishonest employees attempting to access the organization's data center	Exploiting unauthorized access and information into the system, obtaining sensitive information and modifying existing information.	High	High	High
Limited procedures for data recovery plan implementation	Server failure leading to unavailability of all Libyana services	Low	Low	Low

Vulnerability Identification

Vulnerability management is actually a procedure to ensure that your corporate network is secure against potential vulnerabilities, which can open the door to hacker attacks. The security risk appears at the intersection of the vulnerability and the external threat. Identifying potential sources of vulnerability information is the process of identifying a vulnerability. The identified threat vulnerabilities are assessed based on open-source vulnerabilities and other identified vulnerabilities for organizations with similar mission/business processes.

Vulnerability	Severity
Data breach due to tampering and theft of confidential information stored in Libyana servers	High
Fire would activate sprinkler system causing water damage & compromising the availability of Libyana.	High
Exploitation of passwords in script & initialization files	High
Weak Passwords vulnerability leading to brute force attacks for Libyana website or internal systems.	Very Low
Exposing data to risk of unauthorized disclosure through privilege escalation. Executing unauthorized functions in the database	Very High
Attackers exploit vulnerability of SSL protocol by injecting payload within the security protocol itself that is used to protect Libyana business application	High
Attackers will be able to obtain all available communication through incoming and outgoing traffic within the network after reconnaissance process on the Libyana network.	High
Exploiting unauthorized access and information into the system, obtaining sensitive information and modifying existing information.	Very High
Upload of dangerous file types through exploitation of unsecure platforms (email) for critical information flow across all three tiers	Very Low
Use of generic Libyana accounts and Compromise of unexpired/unchanged passwords	High

Risk Determination

In determining risk associated with X, the following formula is used:

- Risk = Threat Likelihood x magnitude of Impact

Appendix E shows the relationship between the threat likelihood and magnitude of impact in determining risks.

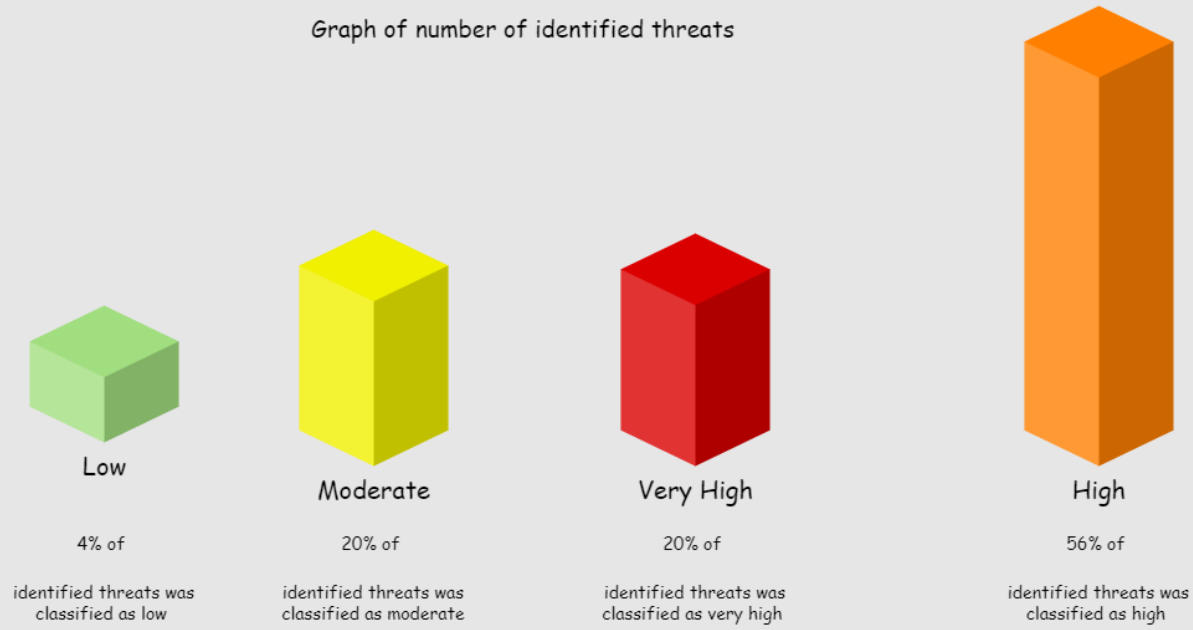
Threat sources	Threat Event	Vulnerability	Overall Likelihood	Level of Impact	Risk
Absence Of Two-Factor Authentication in Libyana payment mechanisms	Identify theft through user impersonation where attacker obtains sensitive resources such as credit card details of the impersonated user	Exploiting unauthorized access and information into the system, obtaining sensitive information and modifying existing information.	Very High	High	High
Absence Of Server Room Security Policy	Conduct physical attacks on organizational facilities	Unrestricted employee access to the server room vulnerability threatens confidentiality, integrity and availability of critical information security systems	High	High	High
Wet-pipe sprinkler system in Libyana Data Center	Fire would activate sprinkler system causing water damage & compromising the availability of Libyana	Fire would activate sprinkler system causing water damage & compromising the availability of Libyana.	Moderate	High	Moderate
Spyware/malware authors use Of automated update setting for operating systems	Denial Of Service (DoS) attack through automatic updates. Effects resources available in induvial user accounts and operating systems	Weak Passwords vulnerability leading to brute force attacks for Libyana website or internal systems.	High	Very High	Very High
Spyware/malware authors use Of automated update setting for operating systems	Insert untargeted malware into downloadable software	Attackers will be able to obtain all available communication through incoming and outgoing traffic within the network after reconnaissance process on the Libyana network.	High	High	High
Trusted employees using unsecure communication platforms for business sensitive information flow	Social Engineering techniques used by attackers to gain legitimate access to confidential and private information for the purpose of identity theft	Attackers will be able to obtain all available communication through incoming and outgoing traffic within the network after reconnaissance process on the Libyana network.	Very High	High	High
Trusted employees using unsecure communication platforms for business sensitive information flow	Attacker delivering known malware to internal organizational information systems (e.g., virus via email).	Attackers will be able to obtain all available communication through incoming and outgoing traffic within the network after reconnaissance process on the Libyana network.	High	Very High	Very High
Phishers taking advantage of the email platform that implement weak filters	Craft phishing attacks	Attackers will be able to obtain all available communication through incoming and outgoing traffic within the network after reconnaissance process on the Libyana network.	Very High	High	High
Phishers taking advantage of the email platform that implement weak filters	Malware provided in the form of phishing emails to obtain private information such as login and password. Leads to unauthorized access to Libyana systems	Upload of dangerous file types through exploitation of unsecure platforms (email) for critical information flow across all three tiers	High	High	High
Attacker / Weak permissions	Privilege Escalation	Exposing data to risk of unauthorized disclosure through privilege escalation. Executing unauthorized functions in the database	High	High	High

Threat sources	Threat Event	Vulnerability	Overall Likelihood	Level of Impact	Risk
Absence of Server room Security policy (Insiders)	Data breach due to tampering and theft of confidential information stored in Libyana servers	Unrestricted employee access to the server room vulnerability threatens confidentiality, integrity and availability of critical information security systems.	High	Moderate	Moderate
Absence of Server room Security policy (Insiders)	Compromise design. manufacture, and/or distribution of information system components (hardware)	Unrestricted employee access to the server room vulnerability threatens confidentiality, integrity and availability of critical information security systems.	High	Moderate	Moderate
The use of weak encryption techniques between users and Libyana application	Conduct communications interception attacks	Use of unsecure cryptographic hash function algorithms leading to theft/corruption of confidential data	High	Very High	Very High
The use of weak encryption techniques between users and Libyana application	Exposing data to risk of unauthorized disclosure	Use of unsecure cryptographic hash function algorithms leading to theft/corruption of confidential data	High	High	High
High privileged attackers accessing MySQL database	Exposing data to risk of unauthorized disclosure through privilege escalation. Executing unauthorized functions in the database	Unspecified vulnerability in the MySQL Connectors component in Oracle MySQL 5.1.34 and earlier allows remote authenticated users to affect confidentiality and integrity via unknown vectors related to Connector.	Very High	High	High
Attacking Libyana network because of absence of firewall	Network downtime performance due to spreading of viruses or malware	Attackers exploit vulnerability of SSL protocol by injecting payload within the security protocol itself that is used to protect Libyana business application	High	Moderate	Moderate
Hackers detect unsecure protocols	Attackers will be able to obtain all available communication through incoming and outgoing traffic within the network after reconnaissance process on the Libyana network.	Usage of unsecure security protocols such as FTP (File Transfer protocol) for transmission of confidential information within the network	High	High	High
Third party attempting to access the organization's data center	Exploiting unauthorized access and information into the system, obtaining sensitive information and modifying existing information.	Unrestricted employee access to the server room vulnerability threatens confidentiality, integrity and availability of critical information security systems.	Very High	High	High
Dishonest employees attempting to access the organization's data center	Exploiting unauthorized access and information into the system, obtaining sensitive information and modifying existing information.	Unrestricted employee access to the server room vulnerability threatens confidentiality, integrity and availability of critical information security systems.	High	High	High
Limited procedures for data recovery plan implementation	Server failure leading to unavailability of all Libyana services	Data center and backup systems located within Libyana building premises results in exposure of critical information systems to environmental and human-related hazards	Low	Low	Low

Mitigation Recommendations

X has adopted a new method to reduce vulnerabilities and try to mitigate potential threats that could directly or indirectly affect the security components associated with X's business operations, and this method is represented in enacting and setting policies. Appendix B detailed the policies which are established and made in Tier 1 then they will be passed on and implemented to Tier 2 and 3.

Risk Assessment Results



This section summarizes risk assessment results to enable Libyana decision makers to quickly understand risks and respond accordingly.

APPENDIX A

Acceptable Use Policy

Policy

1. General Use and Ownership

1.1. All the proprietary information of X that are stored on electronic and computing devices are protected in accordance with the Data Protection Standard.

1.2. Users are permitted to use the X's information resources only for the purposes of the work they are authorized to perform. Any unauthorized use of the X's information systems and resources such as personal use or on behalf of any third party (such as a personal client, family member, political, charitable, school or other purposes) is strictly prohibited, and the user who violates this will be subject to disciplinary action and/or appropriate legal.

1.3. All computer data generated, received or sent using the X's information systems are owned by the X and are not considered to be owned by the user. The X reserves the right to examine all data for any reason and without notice, for example when there are suspicions of violating these rules or any policies and procedures of the X.

1.4. X employees and third-party users who use or have access to X information should be aware of the current limits of their use of the X's information systems, and are responsible for their use of information systems and any use that is made under their responsibility.

1.5. Giving the right to authorized personnel within X to monitor equipment, systems and network traffic at any time for the purposes of security and network maintenance.

1.6. No user is allowed to exceed the permitted and necessary amount of access to private property information to carry out the job and tasks attributed to him.

1.7. X reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

1.8. It should allow all X users to access only the information systems and processes needed to perform their business tasks.

1.9. Accessing, entering or connecting to server rooms will be allowed only for authorized individuals.

1.10. Accessing, entering or connecting to data centers will be allowed only for authorized individuals.

1.11. Providing server rooms with physical security mechanisms that include security locks that work with fingerprint or iris recognition to prevent unauthorized access.

1.12. Providing data centers with physical security mechanisms that include security locks that work with fingerprint or iris recognition to prevent unauthorized access.

1.13. Movement between company facilities for employees requires an access card that proves the person's validity, while visitors are given an access card that is limited in validity and time.

2. Security and Proprietary Information

2.1. Access Control

2.1.1. All X users should only have access to the information systems and processes needed to perform their business tasks.

2.1.2. Each information system user must obtain authorization from the information system administrator in order to have access to the X information systems.

2.1.3. Allows access to information systems and activation of user accounts for each of the employees, contractors, consultants, temporary workers, or

supplier employees in the event that the person performs services for the benefit of X only.

2.2. Username and Password

2.2.1. All user names and passwords must be stored and distributed to the systems securely.

2.2.2. Each user of any information system must have a unique user name and password.

2.2.3. Common usernames and common and generic usernames should not be used.

2.2.4. The minimum allowed password length is 9 characters.

2.2.5. The user is not allowed to share his username and password with other people under any circumstances. The user shall bear full direct responsibility for all activities that take place through his user account on any of the systems he is permitted to use.

2.3. Third Party Access to X Information Systems

2.3.1. The Director of the Information Security Department should conduct an assessment to determine the potential risks to X's information systems arising from access to them by third parties.

2.3.2. It should be taken into account that the aforementioned evaluation includes the following criteria:

- The type and level of access to be granted to the other party.
- Classification of information systems risks to which access will be permitted.
- The reasons on which access to information systems is granted.
- Reference information about the other party.
- Availability and effectiveness of the controls to be applied to regulate and control the access of the other party.

2.3.3. Third party access to X's information systems is granted based on a formal contract between X and the said party.

2.3.4. The contract must include the following conditions as a minimum:

- Terms and conditions under which access is granted.
- The level of security that is natural and logical to be provided by the (third party) to maintain the confidentiality, integrity and integrity of the X information/data being processed.
- Responsibilities of employees of contractors, consultants or suppliers.

2.3.5. An expiration date for the username shall be specified for Contractor, Consultant and all other third-party employees, provided that it does not exceed the expiry date of the contracted project.

2.4. Remote Access

2.4.1. Grants remote access to the X network using users' login procedures.

2.4.2. Remote access is granted on an as-needed basis and for business purposes only.

2.4.3. X grants remote access only to essential operational needs and documents the justification for such access.

2.4.4. Users with remote access should ensure that their X owned or personal computer or workstation, remotely connected to the X Network, have the following:

- Not connected to any other network at the same time, except for personal networks that are under the full control of that user.
- Includes the latest anti-virus, anti-spyware and firewall software.

2.4.5. The user is responsible for any consequences or negative effects arising from the misuse of access.

3. Unacceptable Use

This policy applies to the employees of X and any third party, whether they are working on a permanent or temporary basis, regardless of their work locations. This policy covers all information system environments that X operates or that X has contracted to operate with a third party.

In the event that any of the X employees or a third party (suppliers, contractors, business partners, etc.) violates this policy, he will be subjected to regular procedures in

accordance with the policies of X, which include - without limitation - the work and workers system, the information crime control system, the electronic transactions system, and others.

3.1. System and Network Activities

3.1.1. It is forbidden to introduce malicious programs (such as viruses, worms, Trojan horses, etc.) into the X's information systems.

3.1.2. It is prohibited to introduce free or shared programs into the X's network, whether downloaded from the Internet or obtained from other media, without authorization from the Dean of Information Technology.

3.1.3. It is prohibited to use the X's information systems to store, process, upload, or send data that could be considered biased (political, religious, racial, ethnic, partisan, etc.) or harassing.

3.1.4. It is prohibited to provide offers, products, items, or services that involve fraud or deception using the X's system resources.

3.1.5. It is forbidden to disclose the passwords used by others to access their accounts or to allow the use of those accounts by third parties.

3.1.6. It is prohibited to conduct a port survey or a security survey of the X's information network or information system unless it is authorized by the Director of Information Security and prior notices have been sent to the concerned persons.

3.1.7. It is prohibited to carry out any form of network monitoring during which data that does not pertain to the host machine of the employee's account is intercepted, unless such activity is part of the authorized job/task of the employee.

3.1.8. It is prohibited to circumvent or circumvent the identification of a user or the security of any host, network or computer.

3.1.9. It is prohibited to use any program / language / command, or send messages of any kind, for the purpose of interfering with or disrupting its ends, any user, through any means, locally or via the Internet / intranet / extranet.

3.1.10. It is prohibited to provide information related to X employees or lists of their names to any parties outside the X without authorization from the concerned authorities inside the X.

3.2. E-mail and Communication Activities

3.2.1. Sending any unsolicited e-mail messages, including sending “junk mail” or other advertising materials to persons who have not specifically requested such material (e-mail SPAM), is prohibited.

3.2.2. Prevent harassment via email, phone, or fax, whether in language, frequency, or volume of messages.

3.2.3. Unauthorized use or falsification of email header information or its contents is strictly prohibited.

3.2.4. It is forbidden to create or edit "chain letters", "Ponzi" or "pyramid schemes" of any kind.

3.2.5. It is strictly forbidden to register and correspond with news groups and blogs (newsgroup SPAM).

3.2.6. X employees should not expect any privacy for anything they store, send or receive via the X email system. The X may monitor messages without prior notice.

3.3. Blogging and Social Media

3.3.1. X values and respects the intellectual property rights (including copyright, design rights, patent rights and licenses for source code for software and documentation) associated with its information systems. Accordingly, it is strictly forbidden to blog or use social media to disclose any intellectual property or any information Special Confidentiality X's Intelligent Security Systems.

3.3.2. Violation of any rights of any person or company protected by copyright, patent or other intellectual property rights, or similar rules and regulations through social media or blogging sites using X systems, or other non-Libyan systems but connected with the information technology environment of the X is prohibited. X.

APPENDIX C

Terms and Definitions

- **X**: It is a trading company that sells medicines and medical equipment.
- **SMTP**: SMTP is an abbreviation of the word Simple Mail Transfer Protocol and is used to send messages and direct them to the specified recipient, as the vast majority of mail servers use this protocol in sending.
- **FTP**: FTP stands for File Transfer Protocol, which is a fast way to transfer files from one computer to another on a TCP/IP network such as the Internet
- **SSL:** A digital certificate that certifies the identity of a website and enables encrypted communication. SSL stands for Secure Sockets Layer, a security protocol that creates an encrypted link between a web server and a web browser.
- **RAR**: refers to risk assessment report which identifies threats and vulnerabilities related X
- **Threat Source**: The intent and method targeted at the intentional exploitation of a vulnerability or a situation and method that may accidentally trigger a vulnerability.
- **Threat Event:** An event or situation that has the potential for causing undesirable consequences or impact.
- **Risk**: Potential harm which pose a real threat to the functioning of various organizations.
- **NIST**: The National Institute of Standards and Technology is a standards laboratory and is an unusual agency for the Department of Commerce in the United States.

The following definition and terms can be found in the SANS Glossary located at: https://www.sans.org/security-resources/glossary-of-terms/.

- **Access**
- **Authentication**
- **Authorization**
- **Malware**
- **Blogging**
- **Spam**
- **Confidentiality**
- **Proprietary Information**
- **Intranet**
- **Extranet**

APPENDIX E

Risk Determination

Security Objective	Potential Impact		
	LOW	MODERATE	HIGH
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information. [44 U.S.C., SEC. 3542]	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity. [44 U.S.C., SEC. 3542]	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information. [44 U.S.C., SEC. 3542]	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Reference: NIST Special Publication 800-30R1, Guide for Conducting Risk Assessments

Table: assessment scale – level of risk (combination of likelihood and impact)

APPENDIX G

NIST Federal Information Processing Standards 199

Table 7: Categorization of Federal Information and Information Systems (NIST 800-60 Volume I Revision 1)