Sift Co.

Group Sift

Risk Management Report

Group Members:

- Muhammad Izham Bin Norhamadi (B032020039)
- Ahmad Sha Herizam Bin Tahir (B032020009)
- Affendy Elyas Bin Azhari Sharidan (B032020024)
- Muhammad Imran Bin Rosli (B032020043)

TABLE OF CONTENTS

1. Introduction

1.1 Organization Background

Sift Co. is a technology company in Malaysia that focuses on e-commerce. Sift Co. business model is a hybrid of consumer-to-consumer marketplace and business-to-consumer. It partners with courier service providers to perform item pickup and delivery from its warehouse and sellers.

1.2 Organization Structure

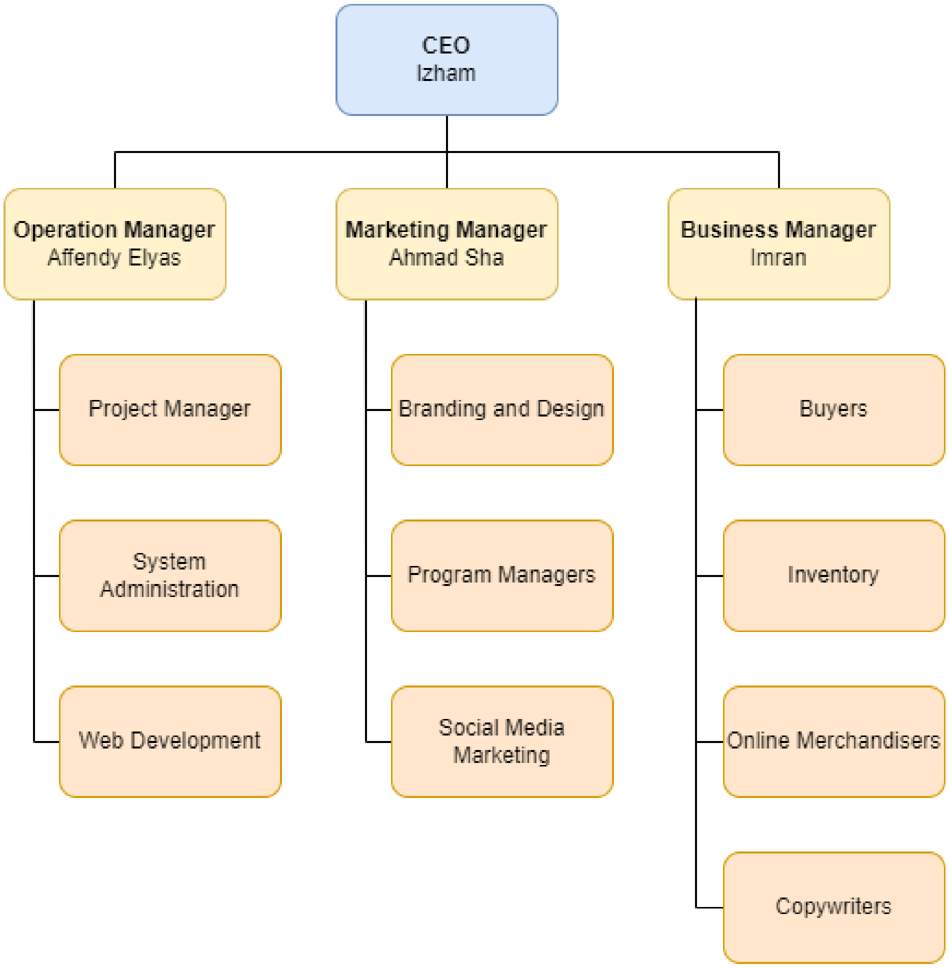


Figure 1.2.1 Organization Structure

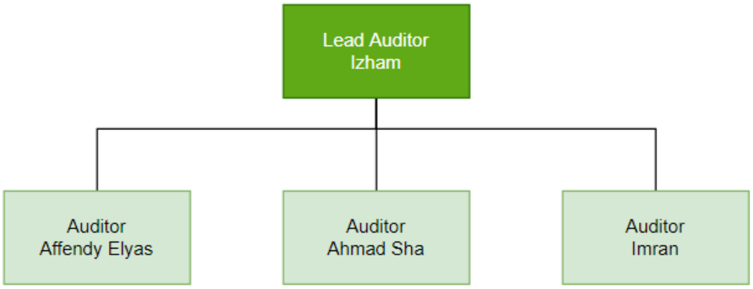


Figure 1.2.2 Board of Auditors

1.3 Network Architecture

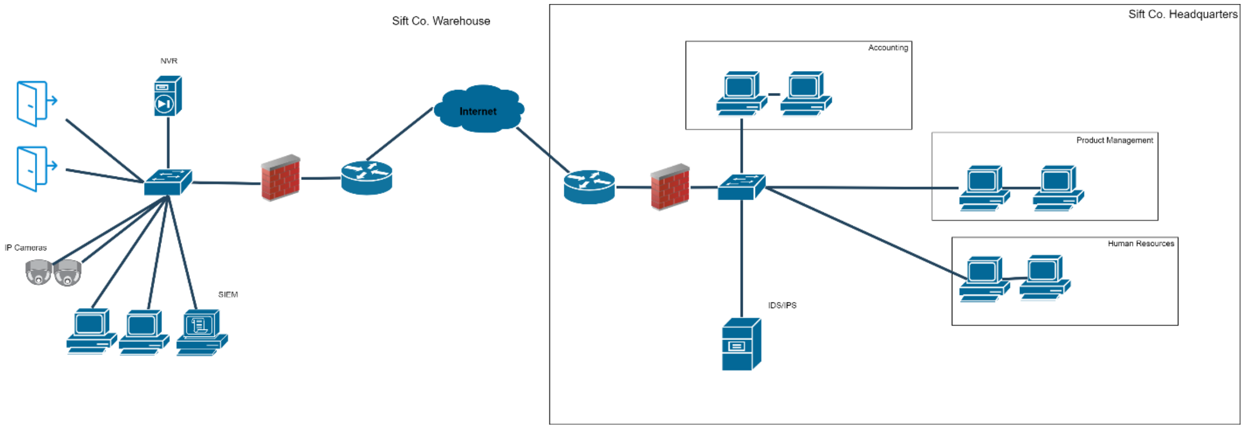


Figure 1.3.1 Network Architecture

1.4 Standard References

ISO/IEC	Title
27005:2018	Information Security Risk Management
27001	Information Security Checklist

ISO/IEC 27005:2008 Information Security Risk Management - enables us to acquire the necessary skills and knowledge to initiate the implementation of an information security risk management process. Therefore, it proves that you can identify, assess, analyze, evaluate, and treat various information security risks faced by organizations. Moreover, it enables you to support organizations prioritize risks and undertake appropriate actions to reduce and mitigate them.

1.5 Scope

To access all relevant assets under which the company functions and its relevance to the information security risk management process, the scope of the security risk management should be defined. The scope of this security risk management audit is to identify the assets and risks in the internal network which is in the Sift Co. headquarters. Since the internal network will be handling a lot of business processes and data there will be more critical assets compared to on-site warehouses.

2. Context Establishment

2.1 Risk Management Process

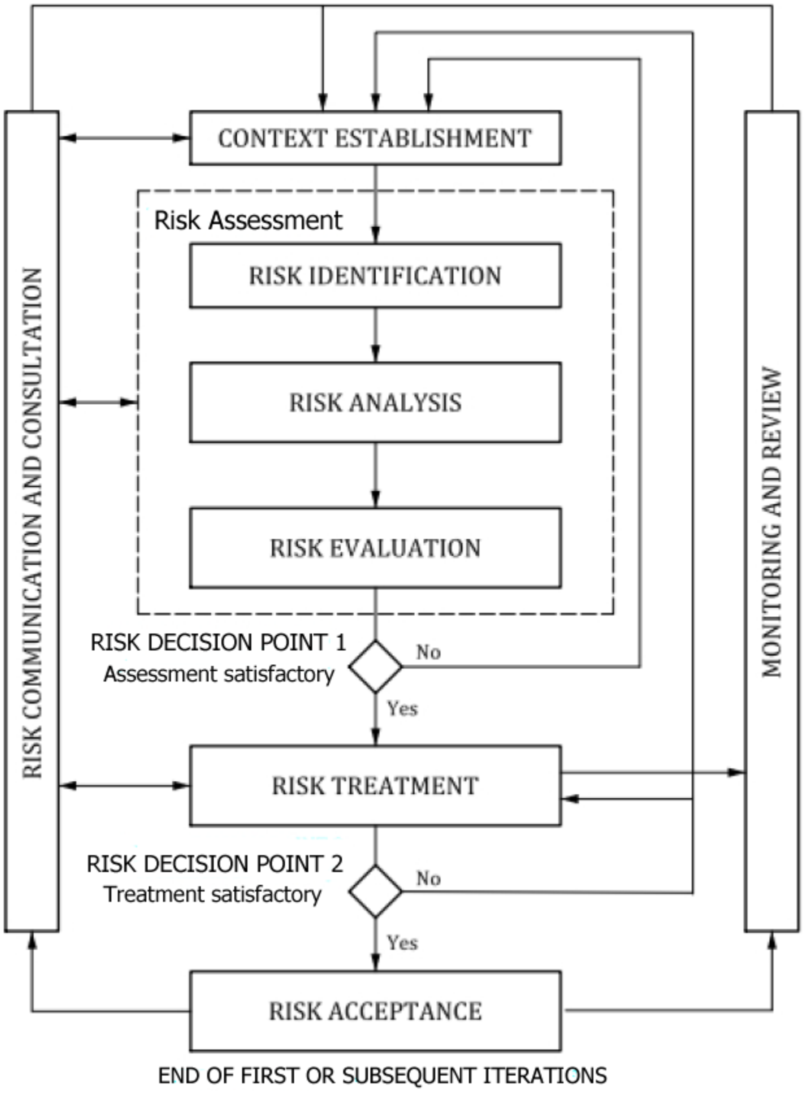


Figure 2.1.1 Risk Management Process

The information security risk management process consists of context establishment, risk assessment, risk treatment, risk acceptance, risk communication and consultation, and risk monitoring and review. The risk management process can be iterative for risk evaluation or risk treatment activities. The iterative approach provides a good balance between minimizing the time and effort spent in identifying controls, while ensuring that high risks are appropriately assessed.

2.2 Basic Criteria

2.2.1 Risk Management Approach

Different approaches can be applied depending on the scope and objectives of the risk management. The approach can be different for each iteration.

An appropriate risk management approach should be selected that addresses basic criteria such as: risk evaluation criteria, impact criteria, risk acceptance criteria.

An organization should access whether necessary resources are available to:

- Perform risk assessment and establish risk treatment plan
- Define policies and procedure with implementation of the controls selected
- Controls monitoring
- Monitor the information security risk management process

2.2.2 Risk Evaluation Criteria

Risk evaluation criteria should be developed to evaluate the organization's information security risk by considering the following:

- The strategic value of the business information process
- The criticality of information assets involved
- Operational and business importance of availability, confidentiality, and integrity

Additionally, risk evaluation criteria can be used to specify priorities of risk treatment.

2.2.3 Impact Criteria

Impact criteria should be developed and specified in terms of the degree of damage or cost to the organization caused by an information security event considering the following:

- Level of classification of the impacted information asset
- Breaches of information security (e.g. loss of confidentiality, integrity, and availability)
- Impaired operations
- Loss of business and financial value
- Disruption of plans and deadlines

2.2.4 Risk Acceptance Criteria

Risk acceptance criteria depend on policies, goals, objectives, and the interests of stakeholders.

To establish risk acceptance scales, the following should be considered:

- risk acceptance criteria can be expressed as the ratio of estimated profit to the estimated risk
- different risk acceptance criteria can apply to different classes of risk
- risk acceptance criteria can include requirements for future additional treatment

Risk acceptance criteria might vary depending on how long the risk is projected to last, such as when the risk is linked to a temporary or short-term activity. The following should be considered while developing risk acceptance criteria:

- business criteria
- operations
- technology
- finance
- social and humanitarian factors

To be considered as an acceptable risk, it must follow the criteria:

- All avoidable risks shall be avoided
- Risks shall be reduced wherever practicable
- The effects of events shall be contained within the site boundary
- Further development shall not pose any incremental risk

3. Information Security Risk Assessment

3.1 General description of information security risk assessment

Risk assessment determines the value of the information assets, identifies the applicable threats and vulnerabilities that exist, identifies existing controls and their effect on the risk identified, determines potential consequences, and prioritizes the derived risks.

3.2 Asset Identification

An asset is something of worth to the company that must be safeguarded. It's important to remember that an information system is more than just hardware and software when it comes to asset identification. The asset identification process should be done to a standard of depth that gives enough information for the risk assessment. The amount of information acquired during the risk assessment is influenced by the level of detail utilised on asset identification. The level can be fine-tuned in subsequent risk assessment rounds.

Critical Asset Level determines the crucial assets that are needed for business continuity ranging from:

Low: Optional asset to ease workload

Medium: Required for business continuity but can receive occasional downtime

High: Required to be running at all times to avoid disruption of all business processes

Asset		Operating System	Type	Location	Num of Copies	IP Address	Owner	Responsible Personnel	Critical Asset Level
1	Payment System Application Server	Windows Server 2019	Hardware, Software	Accounting Department	2	192.168.101.11		Ahmad Marketing Manager	High
2	Product Database	Windows Server 2019	Hardware	Product Management Department	2	34.124.186.51		Imran Business Manager	High
3	Web Server	Ubuntu Server	Hardware, Software	Product Management Department	1	34.124.186.53		Imran Business Manager	High
4	Transaction Database	Windows Server 2019	Hardware	Human Resources Department	2	192.168.101.13		Ahmad Marketing Manager	High
5	Staff Database	Windows Server 2019	Hardware	Human Resource Department	1	192.168.101.15		Affendy Operation Manager	High
6	Email Server	Windows Server 2019	Hardware, Software	Human Resources Department	1	192.168.101.16		Affendy Operation Manager	Low
7	SolarWinds Intrusion	Windows Server 2019	Software	Network Server Rack	1	192.168.101.100		Izham CEO	Medium

Asset		Operating System	Type	Location	Num of Copies	IP Address	Owner	Responsible Personnel	Critical Asset Level
	Detection Software								
8	Router	Cisco 1941	Hardware	Network Server Rack	1	10.10.0.1	Affendy Operation Manager	Affendy Operation Manager	High
9	Policy	-	Operational	Headquarter	1	-	-	Izham CEO	Low
10	Standard Operating Procedure	-	Operational	Headquarter	1	-	-	Izham CEO	Low

3.3 Risk Analysis

3.3.1 Threats Identification

The threat identification procedure looks at IT flaws and evaluates how dangerous they are to the system. It's an important part of company's risk management strategy. Identifying threats allows the company to take preventative measures.

		How long can organization continue without it	Impact of asset absence	Vulnerabilities	Contingency in case of disaster

1	**Hardware (IT only)**	3 days	Business production will get slower than usual	SPOF	All business procedures need to be manually documented by hand
2	**Software**	3 days	Business production will get slower than usual	Cyberattacks	Restart the system, Recover and restore backup data from backup server
3	**Facility**	0 day	Business production cannot be held	No security parameter to protect equipment	Look for new small facilities immediately to do basic emergency business recovery
4	**Personnel**	0 day	No manpower to keep business ongoing	SPOF	Try to recruit staff immediately
5	**Raw Materials**	30 days per batch	None until stock expired	Lack of suppliers	Search for backup suppliers
6	**Transportation System**	30 days per batch	No deliveries of raw materials	Location of headquarter	Find third-party transportation company
7	**Utilities**	0 day	IT Equipment cannot work, lacking daily necessities	No backup water supply and power generator	none

3.3.2 Vulnerability Identification

Vulnerability identification is essential for proactively protecting computer system rather than reacting to an attack. Vulnerability identification method can be used to find and understand flaws in the system, its underlying infrastructure, support systems, and important applications. It gives the ability to assess the risks posed by supply chain and business partners.

When vulnerabilities go undiscovered, attackers can use them to harm applications, generate a denial-of-service attack, or set the stage for a breach. Attackers take use of flaws in software to steal secret and proprietary information that is critical to the company's operations and reputation.

Risk Matrix

Ease of Exploitation \ Impact	Low	Medium	High
Easy	Low	Medium	Critical
Medium	Low	Medium	Medium
Hard	Low	Low	Low

Vulnerability		Type	Affected Resources	Risk Rating
1	Unprotected Server Storage	Hardware	Server	Low
2	No continuation plan for hardware failures	Operational	Server and System	Critical
3	Unprotected email communication line	Software	Private information	Medium
4	CVE-2021-1732: Windows Win32k Elevation of Privilege Vulnerability	Software	Windows Server	Critical
5	CVE-2021-24078: Windows DNS Server Remote Code Execution Vulnerability	Software	Windows Server	Critical

Vulnerability		Type	Affected Resources	Risk Rating
6	CVE-2021-1721: .NET Core and Visual Studio Denial of Service Vulnerability	Software	Windows Server	Critical
7	Unnecessary services running in the background	Software	Windows Server	Low
8	CVE-2021-44228: Apache Log4j2 JNDI features do not protect against attacker-controlled LDAP and other JNDI related endpoints	Software	Web Server	Critical
9	Unnecessary high privileges than required for staff	Operational	Server and System	Medium
10	Lack of back-up copies	Operational	Server	Medium
11	Usage of outdated software	Software	System	Medium
12	Poor password management	Software	Server and System	Critical
13	Single point of failure	Network	Router	Medium
14	Unsupervised work by outside or cleaning staff	Operational	Server and System	Low

3.4 Risk Evaluation

3.4.1 Assessment of Impact

Impact assessment is an evaluation that should be compatible with the established external and internal information security risk management framework and take into consideration the organization's objectives and stakeholder perspectives when making choices. The risk evaluation activity's decisions are mostly based on the acceptable degree of risk. Multiple low or medium hazards combined can result in considerably larger total dangers, which should be addressed.

Severity of Impact evaluates the impact of compromised assets towards business:

Low: Minor to no disruption to business continuity

Medium: Medium disruption to business continuity

Critical: Business-wide disruption that halts most if not all business operations

Incident/Threat Scenario		Affected Resources	Severity of Impact	Impaired Operation
1	System failure due to server overheating	Server	Critical	Most business operations are on hold for at least several hours
2	Compromised system	Server	Critical	Loss of sensitive business data and integrity of systems
3	DDoS attack	Website	Medium	Website will be unavailable for access
4	Natural disaster (flood)	Server	Critical	Servers will be inoperational for a period of time
5	Accidental file deletion	Share media file	Medium	Data could be lost but can be restore from backup
6	Man-In-The-Middle Attack	Email Server	Medium	High vulnerability of confidential information
7	Staff abuse of system privileges to commit misdeeds	Server and System	Medium	Loss of sensitive business data
8	Espionage	Confidential data	Medium	Loss of sensitive business data
9	Business competitor overtaking market	Financial	Low	Reduced business income
10	Theft of Media	Server and System	Medium	Loss of valuable asset
11	Network disruption	Router	Critical	Business operations halted

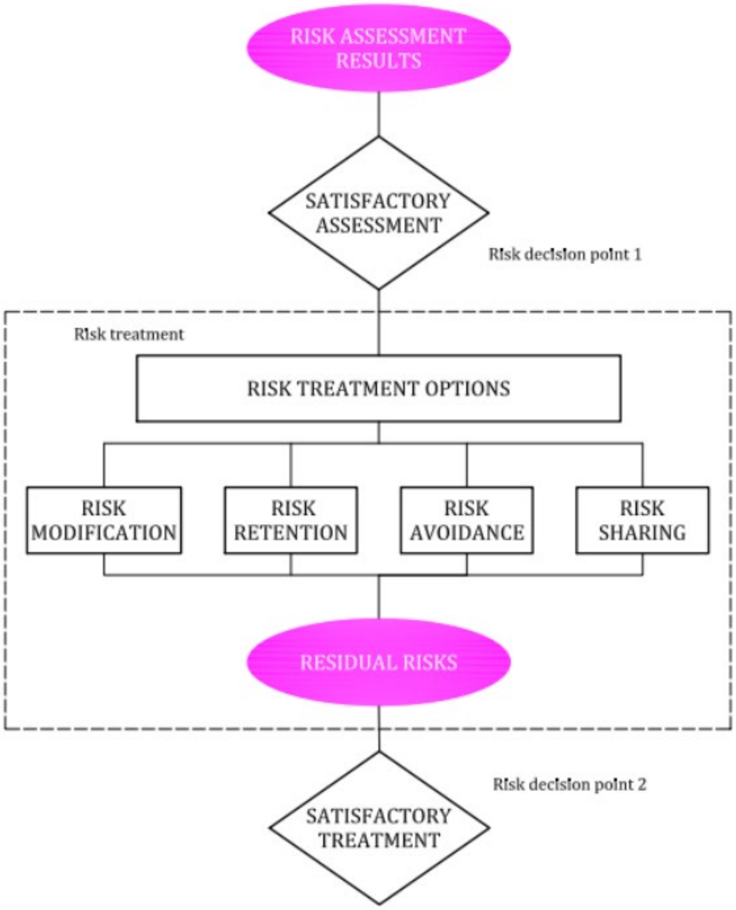
		Likelihood				
		Rare	Unlikely	Possible	Likely	Certain
Impact	Critical	1,4	11	2+8		
	Major					
	Moderate		3	5+7,6,10		
	Minor					
	Insignificant		9			

Table 3.4.1.1 Incident Likelihood to Impact

4. Information Security Risk Treatment

4.1 General Description

Risk treatment may be divided into four categories: risk modification, risk retention, risk avoidance, and risk sharing.



The result of the risk assessment, the estimated cost of adopting these alternatives, and the expected benefits from these options should all be considered when choosing risk treatment solutions. When considerable risk reductions can be achieved at a relatively modest cost, such solutions should be used. Additional improvements may be uneconomical, and judgement must be used to determine if they are justified. The four risk-reduction approaches are not mutually exclusive. A combination of alternatives, including decreasing the likelihood of risks, reducing their repercussions, and sharing or maintaining any residual risks, can sometimes provide significant benefits to the business.

4.2 Monitoring and Review of Risk Factors

Risks are not static. Threats, vulnerabilities, likelihood or consequences can change abruptly without any indication. Therefore, constant monitoring is necessary to detect these changes. This can be supported by external services that provide information regarding new threats or vulnerabilities.

Organization should ensure that the following are continually monitored:

- New assets included in risk management scope
- Necessary modification of asset values due to changed business requirements
- New threats that can be active both outside and inside organization that have not been assessed
- Possibility that new or increased vulnerabilities can allow threats to exploit
- Increased impact or consequences of assessed threats, vulnerabilities and risks
- Information security incidents

Risk monitoring activities should be repeated regularly and the selected options for risk treatment should be reviewed periodically. The outcome of this being continual alignment of the management of risks with the organization’s business objectives, and with risk acceptance criteria.

4.3 Risk Treatment Plan

RISK IDENTIFICATION		RISK TREATMENT	
Event		Action	Plan
1	System failure due to server overheating	AVOID	1. Keep server on cooling rack to allow proper air flow 2. Install self-contained air conditioner mounted close to the ceiling
2	Compromised System	REDUCE	1. Provide scheduled patches to servers 2. Keep IPS up to date 3. Create backup plan and copy for critical data
3	DDoS Attack	AVOID	1. Implement DDoS response plan: • Clear procedure on how to react to DDoS attack • How to maintain emergency business operation 2. Install high level network security such as Firewall and IDS
4	Natural Disaster (flood)	ACCEPT	1. Build a physical barrier around the server to not let the flood get in
5	Accidental file deletion	AVOID	1. Install backup server 2. Recover any accidental deletion of file
6	Man-In-The-Middle Attack	AVOID	1. Set strong router login credential 2. Use HTTPS for business websites 3. Use VPN for any exchange sensitive information
7	Staff abuse of system privileges to commit misdeeds	REDUCE	1. Practice a mandatory business activity engagement for all staff 2. Provide an anonymous form of complaint activity

8	Exploitation of unpatched Windows Server vulnerabilities to gain root access	REDUCE	1. Provide security patches to Windows Servers from Microsoft 2. Disable unnecessary background processes
9	Competition from other business companies	ACCEPT	1. Background checking for possible espionage 2. High restriction on hiring new personnel.
10	Theft of media	ACCEPT	1. Strategic placement of server will hinder unauthorized access 2. Track incoming and outgoing access to server room
11	Network Disruption	REDUCE	1. Invest and improve network equipment and cabling 2. Create a proper maintenance schedule for router

5. Conclusion

Risk management is a critical procedure that managers must keep in place in their organizations. Risks are unavoidable, and managers should develop stronger risk management solutions. The ability to handle risks is critical to an organization's long-term existence. Managers have been obliged to focus on maintaining a solid risk management report by developing values as global marketplaces have become more competitive.

Having a detailed and complete risk assessment and evaluation can be crucial to face any threats for an organization. This is because organizations which do not prepare any risk assessments or procedures can lead to catastrophe of an organization which is popularly known as bankruptcy. This will close the business process and may lead to a pile of debt for the owner of the organization. That’s why having a complete risk management report is important and can make sure every personnel within the organization knows how to handle any types of threats that the organization will face.