*Summary Report – Module 2*

*Operational Risks Summary Report*

Version *1.5*

Prepared By: *John Doe [Your Name Here]*

Date: *05/21/2019*

VERSION HISTORY

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Version #** | **Implemented**  **By** | **Revision**  **Date** | **Approved**  **By** | **Approval**  **Date** | **Reason** |
| 1.0 | Simon Cold | 03/10/18 | Kyle Green | 03/12/18 | Document creation |
| 1.5 | John Doe | 05/14/19 | Kyle Green | 05/16/19 | Updated operational risks & employment of new preparer of document (Nicholas Blackshire) |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

TABLE OF CONTENTS

[1 Introduction](#_Toc487790192) 4

[1.1 Purpose 4](#_Toc487790193)

[2 Executive Summary 4](#_Toc487790194)

[3 Detailed Summary 5](#_Toc487790195)

[3.1 *List of Operational Risks for Each Business Unit* 5](#_Toc487790196)

[3.2 *Description of Operational Risks*  6-](#_Toc487790197)10

[3.3 *Description of Possible Outcomes*  11-](#_Toc487790198)15

[4 Recommendations 16](#_Toc487790199)

[5 SuggEstED aCTIONS 17](#_Toc487790200)

[Appendix A: Approval 18](#_Toc487790201)

[APPENDIX B: REFERENCES 19](#_Toc487790202)

[APPENDIX C: KEY TERMS 20](#_Toc487790203)

# 

# Introduction

## Purpose

This Summary Report provides a summary of the risk identification section of the XYZ Technology Services Risk Assessment Form. Additionally, this Summary Report offers recommendations for the creation of a risk assessment team.

# Executive Summary

XYZ Technology Services is using this Summary Report to address threats to the company. The detailed summary provides information regarding operational risks and the various consequences for these risks. Each department contains unique risks capable of impacting the company’s reputation, finances, productivity, and security. Within this section of the Summary Report, visual diagrams are present to offer more clarity on this important matter. Before we can implement countermeasures for these risks, we must first identify them.

The last sections of the Summary Report deliver recommendations and suggestive actions. In regards to risk, the recommendations in this document are to create a risk assessment team to evaluate and fix operational threats. Furthermore, departments should make sure they comply with policies and effectively train employees. Under the suggested actions section of the Summary Report, are a list of department/role duties. These duties focus on addressing and mitigating risk for each department.

# Detailed Summary

## XYZ Technology Services has five main business units (Departments) which are Accounting, Human Resources, Information Technology (IT), Manufacturing, and Sales & Marketing. The IT department contains two additional business units, which are Application Development and Network Administration. Each unit contains specific operational risks.

## *List of Operational Risks for Each Business Unit*

## *Image of Business Units and Operational Risks*

## 

## *Description of Operational Risks*

## *Accounting*

## Accounting data is hacked due to ransomware:

This type of operational risk involves ransomware, which is malware. There are various ways for this attack to happen. For example, an accounting associate can accidentally click on a phishing email or infected website, which may grant cybercriminals access to the company network. These malicious individuals could then use the ransomware software to prevent us from accessingour important accounting data. We would have to go through loops and hurdles to regain access to our data.

## External fraud on accounts payable:

Accounts payable is an important sector of accounting vulnerable to deceptive expense reimbursements, check tampering, false billing, and much more. It’s important that we employ accounting individuals and third-party vendors we can trust. An External fraud example may include fake vendor accounts, which siphon money from the company.

## Poor accounting documentation:

Poor accounting documentation can include neglecting to document or deficiently documenting important accounting procedures. These procedures are meant to provide instructions on how accountants should perform their duties. For example, accounting documentation could include information about accounting compliance regulations.

## Error of commission:

Accounting consists of data entry, where accuracy is key. This type of error happens when an accountant debits or credits the incorrect account, with the correct value. Sometimes an error of commission can be hard to detect because the total debits and credits will appear equal. However, in reality**,** these accounts are falsely represented.

## *Human Resources*

## Poor compensation package:

Employees desire a reasonable compensation package for their services. A poor compensation package may include no medical coverage, no dental insurance, or discouraging salaries. Although one or more of the above items could probably be present, a company should offer a suitable compensation package for its employees. Workers expect various benefits from their company, in exchange for their daily services.

## Failing to comply with local or international labor regulations:

Specific rules are in place for companies to follow to ensure the safety of employees. Failing to comply with labor regulations could occur for numerous reasons. For example, company facilities could be unsafe (Dangerous design, lacking in safety equipment) and unclean. Other labor issues could include employing illegal workers or overworking employees.

## Outdated EPL (Employment practices liability insurance):

The company should have current EPL coverage to protect against employee conflicts. An outdated EPL may lack important insurance coverage. The company’s disciplinary and termination employee procedures should comply with the EPL insurance, to mitigate risks.

## Improper training on data access:

Employees need consistent training for data access. The IT department may alter the network infrastructure, which can impact all departments. Improper training on data access promotes dangerous and unethical employee behavior. This type of irresponsible training can ignore the importance of strong passwords, understating access levels, and the company policy on personal devices.

## *IT*

## Asset management risk (Misplaced or lost IT devices):

The IT department contains many devices, new and old. Inventorying these devices is essential to prevent unnecessary problems. Asset management risk can occur due to undocumented devices, which could be lost, damaged, stolen, or illegally sold.

## Physical security (Security at datacenter):

Although many of our services are migrating to the cloud, we must still consider physical security. For example, a data center is a physical asset. Protecting this asset requires security guards and security equipment (alarms, cameras, etc.). Physical security becomes a risk if our facilities are vulnerable to physical attacks.

## Audit negligence:

Auditors will evaluate the security of our company, but we cannot guarantee that every Auditor will be thorough. Our odds of risk increase if an Auditor conducts an inefficient examination. An example of audit negligence is when an Auditor discovers a security flawbut forgets to document it or inform the company.

## Budget risk:

Department funding is important for overall productivity. Budget risk can occur due to project deadline issues, bad technological investments, and increased employee turnover rates. Misuse of the IT department budget can be devastating.

## *Application Development (IT)*

## Legacy technology risk:

Maintaining our old or outdated technology is vital, especially if it’s stillfully operational.Legacy technology is a risk primarily because of code flaws and lack of support. Therefore, we should also evaluate the risk or replacing such technology.

## Employee turnover:

Unpredictable events can happen to employees, which impact the company.Developers may decide to leave the company because of personal issues, team complications, injuries, or for other reasons. This risk can also occur in all other departments. The risk of employee turnovers can negatively impact those who still work for the company.

## IDE (Integrated development environment) software fails:

Software Developers depend on IDE software to program. Failing IDE software can occur for many reasons. For example, the IDE could need updating or becomes obsolete. Another factor for failing IDE software includes programming language compatibility issues.

## Database configuration risk:

Databases typically store sensitive data. Therefore, having the correct database configuration is vital. An improper database configuration may involve a bad relational database diagram, confusing labels, and wrong locations for specific data. The database tables, datatype, or information could also be incorrect.

## Bad software QA (Quality Assurance) tests:

Performing QA tests is part of the software development life cycle. Bad software QA tests include not detecting or ignoring code flaws. Additionally, QA testers might forget to document or report their discoveries to their Project Manager.

## Bad front-end coding:

Front-end coding or development normally focuses on visual aspects of an application. Creating a user-friendly design is also important for front-end development. Bad front-end coding can include vulnerable coding, and horrible UIs (User Interfaces).

## *Network Administration (IT)*

## Unused open ports:

Networking devices use various ports to complete a variety of communitive tasks. Unused open ports shouldn’t be accessible for the sake of security. An example could be a device with port 80 (HTTP) or port 443 (HTTPS) open, but this device never connects to or uses the internet.

## Weak privilege and access control:

Employees should only be able to perform their job duties and nothing more! Weak privilege and access control is the opposite of the above statement. For example, some HR employees could contain the same privileges as a Network Administrator. This could cause numerous problems for the entire company.

## No AD (Active Directory) removable media policy:

Active Directory policies provide essential security features. It’s always tempting for employees to bring their own devices into work. The AD removable media policy is responsible for determining which media devices are acceptable on company devices. Without this policy, there are no rules in place for foreign devices, which can plug into company equipment.

## Poor network monitoring:

Network monitoring tools offer security professionals insight into any anomalies occurring on the network. Poor network monitoring is a result of employee negligence. These individuals may ignore to document or recognize suspicious network traffic!

## Weak password policy:

Passwords are an important aspect of security. The company should enforce strong password policies. In contrary, a weak password policy would include short password lengths, repetitious passwords, sharing passwords, and much more.

## *Manufacturing*

## Bad third-party vendor relationship:

Sometimes the company requires third-party vendor assistance for specific products or distribution services. A bad third-party relationship may occur because of trust issues, price issues, or product issues. Maintaining a positive relationship with third-party vendors is healthy for company longevity.

## Emerging markets:

Trends and innovations require manufacturing. However, the decision to perform such manufacturing can become a risky investment. Emerging markets are products on the rise, which require immediate manufacturing. One reason for the urgency is to be first in regards to production.

## Tariff wars (Trade wars):

The importing and exporting of goods is a common procedure for manufacturing companies. Normally, tariff wars occur due to political differences in trading policies. During a tariff war, countries will construct specific importing and exporting rules.

## Safety policy complications:

The work environment should be safe for employees at all times! Safety policy complications may occur because of bad safety policy documentation and rules. Spreading the importance of safety within the workplace is essential.

## *Sales & Marketing*

## Brand risk:

Our brand is what attracts new customers and keeps existing consumers buying. The brand risk might include reputational issues, copyright issues, and relevance issues. Maintaining our brands’ popularity is a constant battle.

## Supply & demand issues:

Supply and demand are classic methods in sales. This can become a risk if we cannot supply our consumers, who may have a high demand for a certain product. The consequences of not having the right balance of supply and demand could be crippling.

## Poor customer service:

Customer support is a crucial aspect of building healthy customer relationships. We must be actively assisting our customers around the clock. Poor customer service might happen if employees demonstrate unethical behavior, invalid guidance, or negligence towards customers.

## Economic crises:

The economy is an important factor, which can dictate the growth of many companies. Therefore, companies should prepare for economic disasters. These disasters include war, famine, protests, and recessions. Although these events are usually out of our control, we should prepare for the worst.

## Pricing complications:

Determining the right price for a product can be tricky. Pricing complications could include products being too expensive or too cheap. Finding the right balance is mandatory because customers have expectations. It’s our responsibility to meet customer expectations with reasonable marketing.

## *Description of Possible Outcomes*

## *Image of Possible Outcome of Risks*

## 

## *Accounting*

## Accounting data is hacked due to ransomware:

The consequences of this risk can be detrimental. A ransomware attack on accounting can make our confidential data inaccessible due to complex encryptions. Furthermore, regaining this data would require negotiations with cybercriminals, resulting in a hefty fee.

## External fraud on accounts payable:

In general, fraud can result in a huge financial loss for the company. External fraud will fill the pockets of criminals stealing company funds and tarnish the victim’s reputation. Consequently, the company may undergo severe investigations.

## Poor accounting documentation:

Poor accounting documentation can create a cluster of problems. Accounting documentation instructs Accountants on proper procedures. Flaws in the accounting documentation can delay audits. Thus, creating additional auditing fees.

## Error of commission:

Accounting data should be correct, to prevent financial problems. The error of commission can produce misleading numerical values within the credits and debits of customer accounts. Improper data entries can cause law suites, terminations, and much more.

## *Human Resources*

## Poor compensation package:

Failing to provide a reasonable compensation package for employees is dangerous. This can increase the employee turnover rate, decrease overall productivity, and hurt our future growth. Why would employees want to sacrifice their hard work for minimal rewards?

## Failing to comply with local or international labor regulations:

Local or international labor regulations protect employees and the company. Failing to comply with these policies can result in audits and penalties. These punishments can even halt all production.

## Outdated EPL (Employment practices liability insurance):

An outdated EPL can produce an abundance of lawsuits. Thus, costing the company millions of dollars. Without this protection, employees can make false claims against the company, such as fake sexual harassment or discrimination statements.

## Improper training on data access:

Improper training on data access opens up a variety of vulnerabilities. Hackers can collect usernames and passwords to obtain unauthorized access. However, hackers are not the only threats to a company. Other employees should not have unauthorized access to systems. This can cause damage to the network!

## *IT*

## Asset management risk (Misplaced or lost IT devices):

Losing track of network devices can decrease security and profits. Furthermore, the inventory sector will have a stressful time ordering and organizing devices. These devices could contain sensitive data, making the company vulnerable to theft of intellectual property.

## Physical security (Security at datacenter):

The consequences of physical security risks include data breaches, property damage, terminations, and investigations. Employees who are on the premises during this event could also be in danger. Physical security should be a top priority for the company.

## Audit negligence:

When an Auditor demonstrates negligence, the entire company is at risk. Audit negligence can produce security vulnerabilities, increasing the odds for exploitations. Moreover, the company will be paying for inefficient auditing.

## Budget risk:

Time and money are factors to consider when you have a budget. The consequences of budget risk can include delays in IT projects, decreases in productivity, and customer relationship issues. Meeting deadlines is an important aspect of IT.

## *Application Development (IT)*

## Legacy technology risk:

Legacy software is a huge risk, potentially introducing new security threats to the company. This software could be difficult to maintain, which will decrease overall productivity and consume company resources.

## Employee turnover:

Employees are the heart of any company. They dedicate their time and qualifications to the company. The risk of employee turnovers can produce developer team complications such as incomplete projects and bad team chemistry. Furthermore, employee turnover rates can discourage the remaining employees!

## IDE (Integrated development environment) software fails:

When IDE software fails, programmers cannot get their work done. This can consume valuable time, requiring developers to find alternative methods for completing complex objectives. Additionally, failing IDE software can impact deadlines and code functionality.

## Database configuration risk:

Incorrect database configurations produce numerous problems. Data could become misplaced, complicating how employees retrieve sensitive information. Vulnerable databases are an invitation to malicious individuals, who want to steal company data.

## Bad software QA tests:

Bad software QA tests could result in vulnerable applications reaching the end-user. Therefore, creating additional security issues such as identity theft. Another consequence of a bad software QA test might include releasing a product that doesn’t even function. The company’s reputation is in jeopardy when a bad software QA test occurs.

## Bad front-end coding:

Bad front-end coding can create web application vulnerabilities, exploitable by cybercriminals. Not only would this impact the visual aspect of an application, but it could also threaten the back-end. Hackers can manipulate the front-end of an application to extract data from databases in the back-end.

## *Network Administration (IT)*

## Unused open ports:

Unused open ports are like doorways for malicious individuals! They will use these ports to obtain network access. From there, havoc will ensue.

## Weak privilege and access control:

Unauthorized users can cause unfixable damage to systems such as restricting everyone from accessing company data. These users could be criminals or employees, but their actions are what is most dangerous.

## No AD (Active Directory) removable media policy:

Without an AD removable media policy, foreign devices will be able to connect to company devices. These foreign objects could contain viruses, which infect the company network. Another consequence of no AD removable media policy is the potential for internal theft.

## Poor network monitoring:

Monitoring network traffic is a primary line of defense against threats. Poor network monitoring allows anomalies to enter the network undetected. As a result, a cyber-attack might occur, which was initially preventable. These attacks can cost the company a lot of money!

## Weak password policy:

A weak password policy allows hackers to steal usernames and passwords with ease. They can accomplish this by implementing various techniques such as brute force or dictionary attacks. Then they would have the ability to imitate employees while causing havoc. Due to weak password policies, the entire network could be in danger.

## *Manufacturing*

## Bad third-party vendor relationship:

Having an unhealthy relationship with third-party vendors can cause product delays, financial disputes, and regulatory violations. The company and the customers can suffer from this risk.

## Emerging markets:

Deciding to invest in emerging markets is a risk in itself. The main consequence of this risk is decreasing profits due to corruption and fraud. Furthermore, we could be violating unknown international laws!

## Tariff wars (Trade wars):

Although we don’t have control over the occurrence of this risk, we should evaluate the consequences of a trade war. Tariff wars can increase the cost of importing and exporting goods. Therefore, hurting the company financially and making it difficult to acquire certain products.

## Safety policy complications:

A bad safety policy can produce high employee turnover rates and high chances for employee injuries. Without a resilient safety policy, we can expect to encounter many lawsuits.

## *Sales & Marketing*

## Brand risk:

The consequences of brand risks include rebranding issues and declining company value. Competitors might see this as the perfect opportunity to eliminate their oppositions.

## Supply & demand issues:

Complications with meeting the supply and demand for products can create consumer conflicts. Products might fail to arrive in time or even become obsolete. This impacts the company’s finances, reputation, and growth.

## Poor customer service:

Poor customer service produces countless issues. These problems can include customer complaints, loss of profits, lawsuits, and regulatory violations.

## Economic crisis:

Similarly to tariff wars, an economic crisis is often out of our control. An economic crisis can alter how consumers spend money. Therefore, this risk has the potential to decrease company profits.

## Pricing complications:

Sales & marketing does require psychology, especially to meet customer needs. When prices are too high, the consumer base may decrease because they can’t afford the product. When the prices are too low, they could assume the quality of the product is not good. This risk can easily impact the company’s financial decisions and survival.

# Recommendations

XYZ Technology Services should construct a risk assessment team to address threats to the company. An effective risk assessment team should include leaders and technical experts. For example, Leadership roles may include a CIO (Chief Information Officer), Risk Assessment Manager, and managers in each department. Technical roles may include Security Analysts and Malware Analysts. Risk assessment leadership roles in every department provide supervision on security procedures. Other recommendations include verifying that each department complies with regulations, and properly trains employees.

# SuggEstED aCTIONS

## *CIO*

* Communicate with Risk Assessment Manager
* Make all final decisions in regards to risk

## *Risk Assessment Manager*

* Communicate with all departments in regards to risk
* Create risk assessment procedures (Call tree, countermeasures)
* Report findings (Risks) to CIO

## *Accounting Tasks*

* Report findings (Risks) to Risk Assessment Manager
* Verify that accounting documents are valid
* Comply with accounting policies
* Train employees on proper accounting
* Stay within the budget

## *Human Resources Tasks*

* Report findings (Risks) to Risk Assessment Manager
* Verify EPL insurance is current
* Maintain a healthy employee compensation package
* Spread safety and security awareness
* Stay within the budget
* Comply with regulations

## *IT Tasks*

* Report findings (Risks) to Risk Assessment Manager
* Meet deadlines
* Stay within the budget
* Train employees on technical procedures (Network Monitoring, Coding, etc.)
* Spread security awareness
* Comply with regulations

## *Manufacturing Tasks*

* Report findings (Risks) to Risk Assessment Manager
* Stay within the budget
* Comply with regulations

## *Sales & Marketing Tasks*

* Report findings (Risks) to Risk Assessment Manager
* Comply with regulations
* Stay within the budget
* Train employees on effective marketing strategies

Appendix A: Approval

The undersigned acknowledge they have reviewed the aboveand agree with the approach it presents. Changes to thiswill be coordinated with and approved by the undersigned or their designated representatives.

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | Generated signature | Date: | 05/16/2019 |
| Print Name: | Brent Tucker |  |  |
| Title: | CEO |  |  |
| Role: | The CEO makes the final decision on major corporate decisions. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | Generated signature | Date: | 05/16/2019 |
| Print Name: | Gary Bishop |  |  |
| Title: | CISO |  |  |
| Role: | The CISO is responsible for determining what security features the company needs. |  |  |

|  |  |  |  |
| --- | --- | --- | --- |
| Signature: | Generated signature | Date: | 05/16/2019 |
| Print Name: | Ira Dixon |  |  |
| Title: | Risk Assessment Manager |  |  |
| Role: | The Risk Assessment Manager confirms and evaluates all risks to the company. |  |  |

APPENDIX B: REFERENCES

The following table summarizes the documents referenced in this document.

|  |  |  |
| --- | --- | --- |
| **Document Name and Version** | **Description** | **Location** |
| **Risk Register version 1** | The Risk Register is a risk assessment form. This form contains risk identification data, risk evaluation data, and risk control information. | C:\Users\Gamer1\Desktop\Security Risk Assessment |
| **Kenton, W. (2019).** | This document provides a thorough explanation of CEO responsibilities. | <https://www.investopedia.com/terms/c/ceo.asp> |
| **Kenton, W. (2019).** | A descriptive explanation of CISO responsibilities. | <https://www.investopedia.com/terms/c/ceo.asp> |
| **Department of Homeland Security. (2019).** | This document provides information about ransomware. | <https://www.us-cert.gov/Ransomware> |
| **Untapped Editorial Team. (2018).** | This is a guide to preventing accounts payable fraud. | <https://www.mediusflow.com/en/untapped/articles/process/how-to-detect-fraud-accounts-payable> |
| **Playaccounting. (2019).** | This document offers a definition and explanation of error of commission. | <https://www.playaccounting.com/explanation/re-exp/error-of-commission/> |
| **Nationwide. (2019).** | This document provides information on EPL insurance. | <https://www.nationwide.com/business/insurance/employment-practices-liability/> |
| **Amadeo, K. (2019).** | This is a descriptive document on trade wars. | <https://www.thebalance.com/trade-wars-definition-how-it-affects-you-4159973> |

APPENDIX C: KEY TERMS

The following table provides definitions for terms relevant to this document.

|  |  |
| --- | --- |
| **Term** | **Definition** |
| EPL (Employee Practices Liability Insurance) | EPL is insurance coverage to employers against claims made by employees. These claims include discrimination, wrongful termination, and harassment. |
| IDE (Integrated Development Environment) | An IDE is a software application with all the necessary features for a Software Developer to create applications. For example, IDEs usually contain a text editor, project editor, and toolbar. |
| UIs (User Interfaces) | A User Interface is what the end-user interacts with to complete specific computer or machine tasks. |
| Tariff wars (Trade wars) | This war occurs when a nation implements restrictions and strict rules on importing/exporting of goods. As a result, foreign countries impose their own rules against that nation. |
| Malware | Malware is malicious software that is harmful to systems. |
| Ransomware | Ransomware is a type of malware that denies users access to their systems or important files. |
| Phishing | Phishing is a hacker technique useful for gathering personal information. This commonly occurs through suspicious emails or infected websites. |
| Brute Force Attack | A Brute Force Attack is a hacker method for obtaining access to anything with password protection. This attack aggressively tries combinations of usernames and passwords until it breaks in. |
| Dictionary Attack | A Dictionary Attack is a hacker method for obtaining access to anything with password protection. This attack attempts to guess passwords using a word-list. |