**UNIVERSITY OF GLOUCESTERSHIRE**

ABC Small Company

**School of Computing and Engineering**

**Module Guide 2022/2023**

**CT7075 Information Security Management**

**Student ID**

**Date of Submission**

Contents

[Introduction 2](#_Toc122586312)

[ABC Company's Security Roles, Procedures and Management Structures 2](#_Toc122586313)

[ABC Company's Security Roles 2](#_Toc122586314)

[Physical Security Roles 2](#_Toc122586315)

[Cyber Security Roles 2](#_Toc122586316)

[ABC Company's Security Procedures 3](#_Toc122586317)

[Employee Training and Education 3](#_Toc122586318)

[Secure Network and Infrastructure 3](#_Toc122586319)

[Secure Development Practices 3](#_Toc122586320)

[Security Monitoring 4](#_Toc122586321)

[Physical Security 4](#_Toc122586322)

[Data Privacy 4](#_Toc122586323)

[Incident Response Plan 4](#_Toc122586324)

[ABC Company’s Management Structures 4](#_Toc122586325)

[Network Diagram 5](#_Toc122586326)

[Risk Analysis Framework 6](#_Toc122586327)

[Risk Identification 6](#_Toc122586328)

[Risk Assessment/ Evaluation 7](#_Toc122586329)

[Risk Mitigation 7](#_Toc122586330)

[Risk Monitoring 8](#_Toc122586331)

[Recommendations 8](#_Toc122586332)

[Technical Security Measures 9](#_Toc122586333)

[Human Security Measures 9](#_Toc122586334)

[Physical Security Measures 9](#_Toc122586335)

[Identification and Authentication Technologies 10](#_Toc122586336)

[Business Continuity and Disaster Recovery Plan 10](#_Toc122586337)

[Conclusion 10](#_Toc122586338)

[References 11](#_Toc122586339)

# Introduction

This report will analyze the security posture of ABC Company (company of our choice), a small start-up business providing web development and digital marketing services. The company was founded in 2020 and currently has a staff of ten, including the company's founder and CEO. ABC Company is based in the United Kingdom and serves clients around the world.

The main security threats faced by ABC Company are those related to the web development and digital marketing services it provides. These include malicious actors attempting to access the company's client data, malicious code being injected into their websites, and other cyber-attacks. Additionally, the company's physical security may be at risk from theft or vandalism.

# ABC Company's Security Roles, Procedures and Management Structures

ABC Company has established a security policy which outlines the roles, procedures and management structures for the company. The policy is designed to ensure the security of the company's data and systems, and to ensure compliance with applicable regulations.

## ABC Company's Security Roles

ABC Company’s security roles are divided into two distinct categories: physical security roles and cyber security roles. Each of these roles are essential to the protection of ABC Company’s assets and its customers.

### Physical Security Roles

The first security role is that of the physical security guard. This role is responsible for protecting the company’s physical assets, such as its buildings and equipment, from theft, vandalism, and other unauthorized access. The guard is responsible for controlling access to the premises, monitoring and responding to any suspicious activity, and conducting regular security checks. Additionally, the guard may be required to respond to emergency situations and help prevent criminal activity.

The second physical security role is that of the security manager. This individual is responsible for developing and implementing policies and procedures that ensure the security of the company’s physical assets (Kotter, 1996). The security manager is also responsible for the training and supervision of security personnel, as well as conducting regular security audits. The security manager is also tasked with overseeing the security system and its maintenance.

The third physical security role is that of the security technician. This individual is responsible for installing and maintaining the security system on the premises. The security technician is also responsible for testing the system to ensure it is functioning properly and for responding to any technical issues or problems that may arise.

### Cyber Security Roles

The first cyber security role is that of the network security analyst. This individual is responsible for conducting network security assessments to identify and mitigate any security risks posed by external threats. The analyst is also responsible for developing plans and policies to protect the company’s networks and systems from malicious actors. Additionally, the analyst may be required to respond to cyber incidents and investigate any potential security breaches.

The second cyber security role is that of the security administrator. This individual is responsible for administering and maintaining the security of the company’s networks and systems. This includes developing and implementing access control policies, monitoring access to the network, and responding to security incidents. Additionally, the security administrator is responsible for ensuring the security of the company’s data and for developing and maintaining security procedures (Lambert & Harrington, 2021).

The third cyber security role is that of the security engineer. This individual is responsible for designing, developing, and implementing security systems and processes. The security engineer is also responsible for researching and evaluating new security technologies and for providing technical support to the security team.

ABC Company’s security roles are essential to the protection of its assets and customers. The physical security roles are responsible for protecting the company’s physical assets, while the cyber security roles are responsible for protecting the company’s networks and data. Each of these roles is equally important and must be filled in order for the company to remain secure.

## ABC Company's Security Procedures

ABC Company has developed a comprehensive security plan to ensure the safety and security of its web development and digital marketing services, clients, and employees.

### Employee Training and Education

ABC Company provides regular training and education to all employees on security policy and procedures, including the importance of good password hygiene, secure file sharing and storage, and the use of two-factor authentication. Additionally, the company provides periodic security awareness training to ensure that employees understand the latest security threats and how to protect themselves from them.

### Secure Network and Infrastructure

ABC Company has set up a secure network infrastructure with multiple layers of protection, including firewalls, intrusion detection and prevention systems, data encryption, and authentication (Peltier, 2001). All customer data is stored in a secure database and is encrypted using the latest encryption standards. In addition, the company employs a dedicated IT security team to maintain the network infrastructure and respond to any security incidents.

### Secure Development Practices

ABC Company has implemented secure development practices to ensure that all web development and digital marketing services it provides are secure. This includes code reviews, static analysis, dynamic testing, and secure coding standards. Additionally, the company has implemented automated security scanning tools to detect any vulnerabilities in its web applications.

### Security Monitoring

ABC Company has implemented a comprehensive security monitoring system to detect any suspicious activity or potential threats. This system includes intrusion detection and prevention systems, as well as real-time monitoring of user accounts and activities. Additionally, the company has implemented automated monitoring tools to detect any malicious code or applications that may have been injected into its websites.

### Physical Security

ABC Company has implemented a comprehensive physical security plan to protect the company's premises and employees. This includes the installation of CCTV cameras, access control systems, and security guards. Additionally, all employees are required to wear ID cards at all times, and visitors must be accompanied by an authorized employee at all times.

### Data Privacy

ABC Company is committed to protecting the personal data of its clients. To this end, the company has implemented secure data storage policies and procedures, as well as data encryption technologies. Additionally, the company has implemented a privacy policy that outlines how it will use, store, and protect its clients' data.

### Incident Response Plan

ABC Company has implemented a comprehensive incident response plan to ensure that any security incidents are dealt with in a timely manner. This plan includes a procedure for reporting security incidents, an incident response team, and a process for notifying customers and authorities of any security incidents.

By implementing these security measures, ABC Company is ensuring that its web development and digital marketing services are secure and that its customers' data is protected. Additionally, the company is ensuring that its employees are aware of the latest security threats and how to protect themselves from them.

## ABC Company’s Management Structures

ABC Company’s management structure is based on a combination of centralized and decentralized control. At the highest level, the company’s founder and CEO is ultimately responsible for all strategic decisions, while day-to-day operations are managed by a small but experienced executive team.

At the top of the management structure is the CEO, who sets the overall direction and strategy for the company. They are responsible for hiring and managing the executive team, as well as setting the company’s vision and goals (Berry, 2016). The CEO is also responsible for protecting the company’s interests, ensuring it meets its legal and regulatory obligations, and addressing any external threats to the company’s operations.

The executive team is the core of the company’s management structure. It consists of the company’s CTO, CMO, CFO, and other senior executives, all of whom report directly to the CEO. They are responsible for developing and implementing the company’s strategies, managing day-to-day operations, and ensuring the company meets its goals and objectives (Gueche, 2018). The executive team is also responsible for dealing with any external threats or risks to the company’s operations.

Underneath the executive team is the management team, which is responsible for managing the company’s day-to-day operations. They are typically comprised of the company’s middle managers, who are responsible for overseeing the work of the company’s employees. They manage the company’s resources, ensuring that they are being used efficiently and effectively (Lipman, 2018). They are also responsible for ensuring that the company meets its targets and objectives.

The employees are the last level of the company’s management structure. They are responsible for carrying out the tasks assigned to them by the management team. They are the ones who are responsible for actually delivering the services and products to the company’s clients.

This management structure is based on a combination of centralized and decentralized control. The company’s founder and CEO is ultimately responsible for all strategic decisions, while the executive team and management team are responsible for carrying out those decisions and managing the company’s day-to-day operations. Ultimately, it is the employees who are responsible for actually delivering the services and products to the company’s clients.

Overall, ABC Company’s management structure is designed to ensure that the company is able to meet its goals and objectives, while also ensuring that it is able to respond quickly to any external threats or risks. By combining centralized and decentralized control, the company is able to ensure that the right decisions are made and that the company is able to act quickly when the need arises.

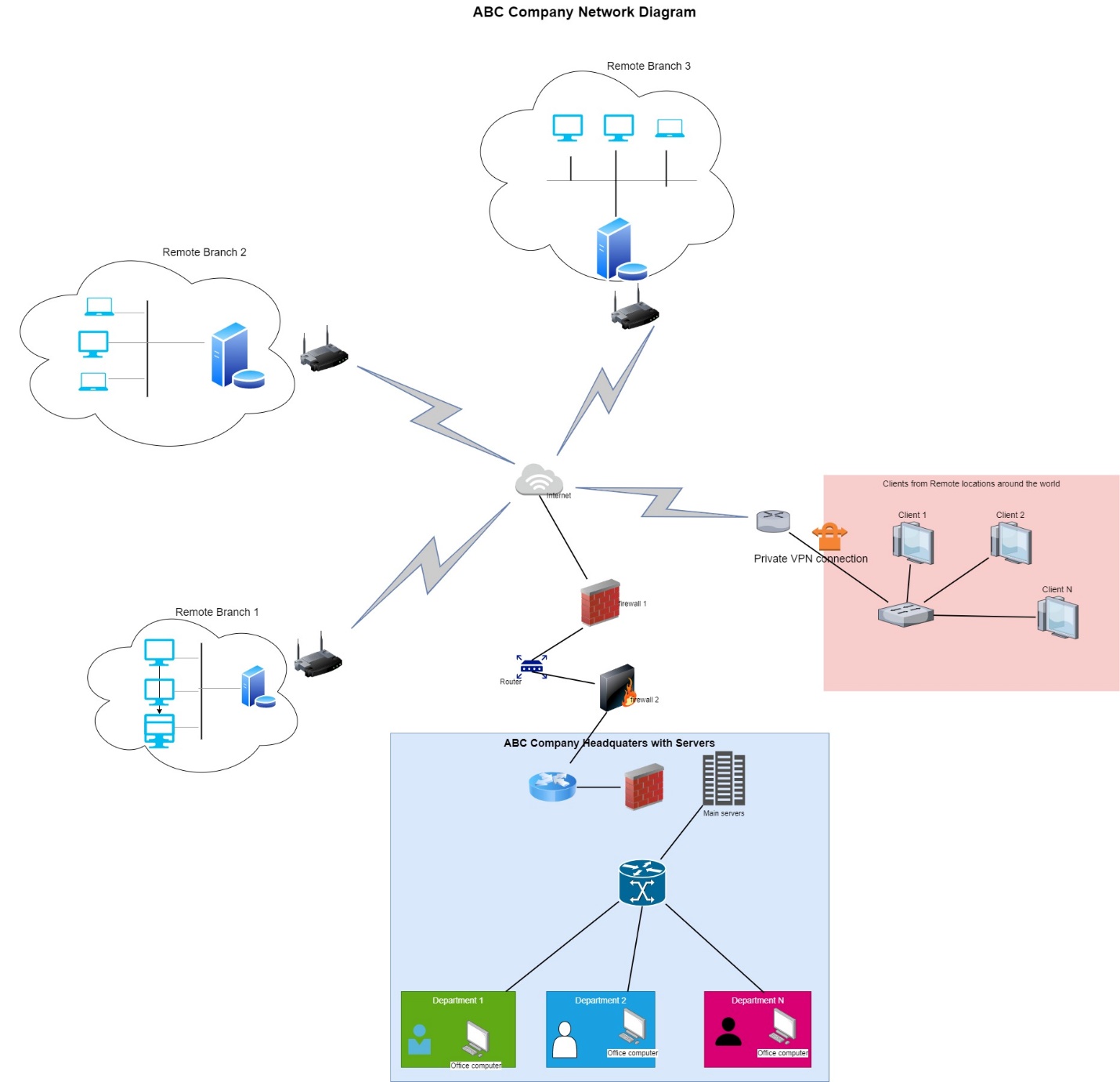
# Network Diagram

The following network diagram depicts the key locations, departments, and devices within ABC Company. The diagram includes the company's headquarters, where the company's servers and IT systems are located, and the company's remote offices, which are located in different countries around the world.

The company's headquarters is connected to the internet via a router, which provides secure access to the company's servers and systems. The headquarters also has a firewall, which is used to prevent unauthorized access to the network. The remote offices are connected to the internet via a secure VPN, which provides access to the company's servers and systems.

The diagram also includes the company's servers and systems, which are located in the company's headquarters. The servers and systems are protected by a firewall, which is used to prevent unauthorized access. The servers and systems are also monitored by the IT manager, who is responsible for ensuring their security.

The diagram also includes the company's clients, which are located in different countries around the world. The clients are connected to the company's servers and systems through secure VPNs, which provide access to the company's services.



# Risk Analysis Framework

Risk analysis is the process of assessing the probability of a particular outcome or event occurring (Holland, 2018). It is used to identify, evaluate and prioritize potential risks and to develop strategies for managing those risks. A risk analysis framework is a systematic process for identifying, analyzing, and evaluating the risks facing a company (NIST., 2020). It is a crucial step in developing a risk management plan, as it helps the company identify potential threats and vulnerabilities, assess their likelihood and impact, and prioritize actions to mitigate or eliminate those risks (Rouse, 2020).

Risk analysis is an important tool for businesses as it helps them to identify and manage risks that could potentially have a negative impact on their operations, profitability and reputation (Chase, Jacobs, & Aquilano, 2006). Risk analysis can also be used to identify and mitigate potential opportunities that may be available to a business.

Risk analysis can be applied to a range of business activities and decisions, such as developing a new product, entering a new market or expanding into a new region (Williams, 2017). Risk analysis can also be used to develop strategies for managing the risks associated with existing activities, such as production and operations, or when making decisions about investments or acquisitions (Friesen, 2016).

ABC Company’s Risk Analysis Framework is a systematic approach used to identify, assess, and manage security risks that could potentially have an adverse impact on the company’s operations. The framework begins with the identification of potential risks and then progresses to the assessment of those risks. The evaluation of the risks is followed by the development of an appropriate risk management plan.

The framework is designed to provide ABC Company with a comprehensive view of its security risks and enable it to develop an effective plan of action to address those risks.

The purpose of this paper is to outline a comprehensive risk analysis framework for ABC Company. The framework will provide an overview of the steps involved in conducting a risk analysis and will discuss the different tools and techniques that can be used to identify and evaluate risks in ABC Company’s. The paper will also discuss the importance of having a risk management plan in place and how to develop one.

Risk analysis is an important part of any organization’s security and safety program, and it is essential for ABC Company to have a risk analysis framework in place to evaluate its key security risks. The following framework provides a detailed overview of the risk analysis process used by ABC Company

## Risk Identification

The first step in the risk analysis process is to identify the risks that ABC Company may face. In order to do this, the company will need to conduct a risk assessment to identify potential threats and vulnerabilities such as malicious actors, as well as threats from internal sources, such as poor security practices. This can be done through analyzing existing threats, conducting research into emerging threats, and reviewing the company’s existing security policies and practices (Gulati, 2020). Additionally, the company can use a risk matrix to help identify areas of risk. Once the risks have been identified, the company should rank them according to their potential impact and likelihood of occurrence. This will help the company to prioritize the risks and allocate resources accordingly.

Alternative steps to be followed to identify risks are as follows. The first step is to identify potential risks. This involves gathering data and information from various sources, such as internal and external stakeholders, financial reports, industry reports, and so on. It is also important to consider the company’s current and past activities, as well as any changes or developments that may have taken place in the environment.

Once the data and information has been gathered, the next step is to analyze the data and identify potential risks. This can be done using a variety of tools and techniques, such as brainstorming, SWOT analysis, or a risk matrix. Brainstorming is a popular tool for identifying potential risks, as it encourages all stakeholders to think of any potential risks, no matter how small or insignificant they may seem.

SWOT Analysis is another popular tool for identifying potential risks. It is used to analyze the company’s internal strengths and weaknesses, as well as external opportunities and threats. By analyzing these four elements, it is possible to identify potential risks that may have a negative impact on the company’s operations, profitability or reputation.

## Risk Assessment/ Evaluation

Once the potential risks have been identified and ranked, the company needs to assess the risks in order to determine their potential impact. This can be done by analyzing the impact of the risks on the company’s operations, assets, and personnel. Additionally, the company should consider the cost of mitigating the risks, as well as the potential impact of not taking action.

Risk assessment involves assessing the probability of each risk occurring and the potential impact it may have on the company’s operations, profitability or reputation. This can be done by using a variety of tools and techniques, such as a risk matrix or impact/probability matrix. A risk matrix is a useful tool for evaluating risks, as it allows the user to assess the probability and impact of each risk on a scale of low to high. This helps to provide a clearer picture of each risk and its potential impact.

The impact/probability matrix is another useful tool for evaluating risks. This involves assigning a probability and an impact to each risk, and then plotting them on a graph. This helps to identify which risks are most likely to occur and which ones have the potential to cause the most harm.

## Risk Mitigation

Once the risks have been identified and assessed, the company needs to develop strategies to mitigate them. First, we need to identify mitigation strategies for each of the identified risks. This includes identifying measures that can be taken to reduce the likelihood of the threat occurring, as well as measures to reduce the impact of the threat if it does occur. This measure includes the preventive measures, such as implementing security policies and procedures, deploying security software, and training staff on security protocols. Additionally, the company can use detective measures to detect threats and vulnerabilities, and corrective measures to respond to and recover from security incidents.

Mitigation strategies involve taking steps to reduce the likelihood of a risk occurring or to minimize its potential impact. This can involve implementing policies and procedures to reduce the risk, such as introducing safety measures or establishing a quality assurance process. It can also involve making changes to existing processes or procedures, such as improving training programs or introducing new technology.

## Risk Monitoring

Once the risks have been identified, assessed, and mitigated, the company needs to monitor and review the security measures to ensure that the mitigation measures are effective and all risks are being managed. This can be done by regularly reviewing the company’s security policies and procedures, monitoring the security software, and assessing the effectiveness of the security measures.

There are several tools and techniques that ABC Company can use in its risk analysis framework, including:

Risk assessment tools: Risk assessment tools, such as a risk matrix, can help the company determine the likelihood and impact of each threat.

Vulnerability assessment: A vulnerability assessment can help the company identify vulnerabilities in its systems and infrastructure that could be exploited by malicious actors.

Threat modeling: Threat modeling involves analyzing the potential threats to a system and determining the likelihood and impact of each threat.

Security assessment: A security assessment can help the company identify weaknesses in its security posture and develop a plan to address those weaknesses.

Overall, a risk analysis framework is an essential component of a robust risk management plan. By following a systematic process for identifying, analyzing, evaluating the risks facing the company and monitor its key security risks, ABC Company can ensure that it is prepared to handle any potential threats and vulnerabilities. This will help the company to protect its assets, personnel, and operations, and ensure that it is prepared to respond to any security incidents.

# Recommendations

Based on the analysis and findings of the previous sections, the following recommendations are made to improve ABC Company's security posture.

## Technical Security Measures

The most effective way for ABC Company to protect its information and data from malicious actors is to implement technical security measures. These measures include firewalls, antivirus software, and other security tools to protect against cyber-attacks. Firewalls are used to control access to and from a network, and can be used to block malicious traffic. Antivirus software can detect and remove malicious code and other malicious software. Additionally, ABC Company can use encryption to protect data at rest, and secure protocols such as SSL/TLS to protect data in transit.

ABC Company should also consider implementing a web application firewall (WAF) to protect against malicious code injection and other web-based attacks. A WAF is a security tool that can detect and block malicious traffic before it reaches the web application. Additionally, ABC Company should consider implementing two-factor authentication (2FA) for access to their services. 2FA requires two separate pieces of information to gain access, such as a username and password, plus a one-time code sent via SMS or email. This adds an extra layer of security and makes it much more difficult for malicious actors to gain access to the system.

## Human Security Measures

In addition to technical security measures, ABC Company should also consider implementing human security measures. These measures can help to protect against malicious actors by making it harder for them to access the system. For example, ABC Company should consider implementing a strong password policy that requires employees to use unique, complex passwords that are changed regularly. Additionally, ABC Company should consider implementing a system of regular security awareness training to ensure that employees are aware of the risks posed by cyber-attacks and know how to respond appropriately.

ABC Company should also consider implementing a process for monitoring user activity. This can help to detect suspicious behavior and prevent malicious actors from accessing the system. Additionally, ABC Company should consider implementing access control measures to ensure that only authorized personnel have access to sensitive data. This can be done through the use of roles-based access control, which assigns different levels of access to different users.

## Physical Security Measures

Finally, ABC Company should consider implementing physical security measures to protect against theft and vandalism. This can be done by implementing the following;

Physical Access Controls - Physical access controls should be implemented to ensure that only authorized users can access the company's premises. This can be done by using access cards, biometric authentication, and other security measures.

Surveillance Systems - Surveillance systems such as CCTV should be implemented to monitor the premises for any suspicious activity. This will help to ensure that any potential threats are identified and addressed in a timely manner.

Security Guards - Security guards should be employed to help protect the premises from any potential threats. This can help to deter any malicious actors from attempting to access the company's premises.

## Identification and Authentication Technologies

To further improve the security of ABC Company’s systems, the company should consider implementing identification and authentication technologies. This can be done through the use of biometric authentication, such as fingerprint or retina scanning. This type of authentication requires a unique biological identifier to gain access to the system, making it much harder for malicious actors to gain access. Additionally, ABC Company should consider implementing single sign-on solutions, such as OAuth and SAML, to allow users to access multiple services with a single login. This makes it easier for users to access the services they need, while also making it more difficult for malicious actors to gain access.

In summary, ABC Company faces a number of security threats, both online and off. To protect against these threats, the company should implement a number of security measures, including technical, human, and physical security measures, and any identification and authentication technologies that would be appropriate. By taking these steps, ABC Company can ensure that its information and data is secure and protected from malicious actors.

# Business Continuity and Disaster Recovery Plan

ABC Company should develop a business continuity and disaster recovery plan to ensure that its operations can continue in the event of a security incident or disaster (Barker, 2019). The plan should include procedures for responding to incidents and disasters, as well as procedures for ensuring that data and systems are backed up and can be recovered if necessary. The plan should also include procedures for notifying clients of any incidents or disasters and procedures for restoring operations once the incident or disaster has been resolved (Governance., 2020).

The plan should also include measures to ensure that the company is able to maintain its operations during an incident or disaster (Microsoft., 2020). This could include the use of redundant systems and backup facilities, as well as measures to ensure that the company's operations can continue in the event of a power outage.

# Conclusion

This report has analyzed the security posture of ABC Company and provided recommendations for improving the company's security posture. It has also outlined a business continuity and disaster recovery plan that the company should develop and implement in order to ensure that its operations can continue in the event of a security incident or disaster. The report has highlighted the importance of implementing technical, human, and physical security measures, as well as any identification and authentication technologies that would be appropriate for the organization to improve their information security.

# References

Barker, J. (2019). *Risk Analysis and Management. .* Retrieved from https://www.thebalancecareers.com/risk-analysis-and-management-4174958

Berry, J. (2016, November 15). *Management structure: How to build the right one.* Retrieved from forbes: https://www.forbes.com/sites/jberry/2016/11/15/management-structure-how-to-build-the-right-one/#63f46b7e97d4

Chase, R. B., Jacobs, F. R., & Aquilano, N. J. (2006). *Operations Management for Competitive Advantage. .* McGraw-Hill. .

Friesen, J. (2016). *Risk Analysis: A Strategic Tool for Business Planning and Management. .*

Governance., I. (2020). *Vulnerability Assessment and Penetration Testing Explained. .* Retrieved from https://www.itgovernance.co.uk/blog/vulnerability-assessment-and-penetration-testing-explained

Gueche, A. (2018). *What is the management structure of a company? .* Retrieved from smallbusiness: https://smallbusiness.chron.com/management-structure-company-2867.html

Gulati, K. (2020). *What is a Risk Analysis Framework and How to Develop One?.* Retrieved from https://www.techopedia.com/definition/33205/risk-analysis-framework

Holland, P. (2018). *Risk Analysis & Risk Management. In The Oxford Handbook of Risk Management. .* Oxford University Press.

Kotter, J. P. (1996). *Leading change. .* Harvard business review.

Lambert, D. M., & Harrington, S. J. (2021). *Risk management in organizations: An integrative approach. .* Wiley.

Lipman, F. (2018). *The benefits of a decentralized organizational structure. .* Retrieved from https://smallbusiness.chron.com/benefits-decentralized-organizational-structure-25185.html

Microsoft. (2020). *Developing a Business Continuity and Disaster Recovery Plan. .* Retrieved from https://docs.microsoft.com/en-us/azure/security/fundamentals/develop-business-continuity-plan

NIST. (2020). *Risk Management Framework Overview.* Retrieved from https://www.nist.gov/cyberframework/risk-management-framework-overview

Peltier, D. (2001). *Risk assessment and management for projects. .* John Wiley & Sons.

Rouse, M. (2020). *Risk Analysis. SearchCIO.* Retrieved from https://searchcio.techtarget.com/definition/risk-analysis

Williams, L. (2017). *Risk Management and Risk Analysis. .* Retrieved from https://www.investopedia.com/terms/r/riskmanagement.asp

Top of Form