**[Network Security Management]**

**Key Contributors:**

**Amechi Nwaeze, Abdul Alqarni, Marcus Harmon, Chris Hyde**



**[10-1-2023]**

# TABLE OF CONTENTS

* Page 3: Executive Summary
* Page 4: Project Milestones
* Page 5: Materials, Deliverables, Accomplishments
* Page 6: Asset Inventory
* Page 7-8: Risk Register
* Page 9: Risk Assessment
* Page 10-11: Secure Controls Framework
* Page 12: Vulnerability Assessment
* Page 13-14: SWOT Analysis
* Page 15: Governance
* Page 16-17: Cyber Hygiene - Privacy Analysis Impact and Business Analysis Impact
* Page 18: Project Management and Github Link
* Page 19: Conclusion
* Page 20: References

# EXECUTIVE SUMMARY The goal of this project is to identify and implement a highly secure, enterprise network that can be identified as a low to middle-end company structure using viable security frameworks, a security-driven business analysis/implementation, and strong security controls and monitoring for risks. A strong network infrastructure that is built and maintained by an organization is only truly secure in the current business landscape when there are the proper policies, management, and security foundations planned when a system and network is designed. Our network can be configured to meet those goals by having a functional design, using network and hardware logs, and by applying the proper risk mitigation strategies according to our security framework. This project can be useful for organizations who are just starting out who need an easy-to-use network structure that they can configure for their own use or for any organization who needs to begin implementing their first security environment in a way that can defend target assets and information or monitor the network properly.

# Project Milestones:

1. Research: Discover which cyber security frameworks, standards, and regulations are most applicable for the team objectives and select the feasible ones considering risk appetite.
2. Initialization: Research/work on building the network of which we wish to defend and mark down any areas of vulnerability or security controls that will need to be considered later. We will include security as needed as the network is being built if framework or policy demands it.
3. Controls/Monitoring: Insert any security controls or logging programs to build the backbone of our secure network.
4. Testing: Attempt a handful of common attacks that can test the controls put in place and to see if log files can properly indicate an attack has happened after inspection.
5. Conclusion: Take notes on testing and repeat any of the prior steps if controls fail or if changes are needed.

Materials:

1. Computer
2. Safe Coding Environment
3. Database
4. Firewall
5. Internet/Network
6. Software Packages
7. Linux Operating System

Deliverables:

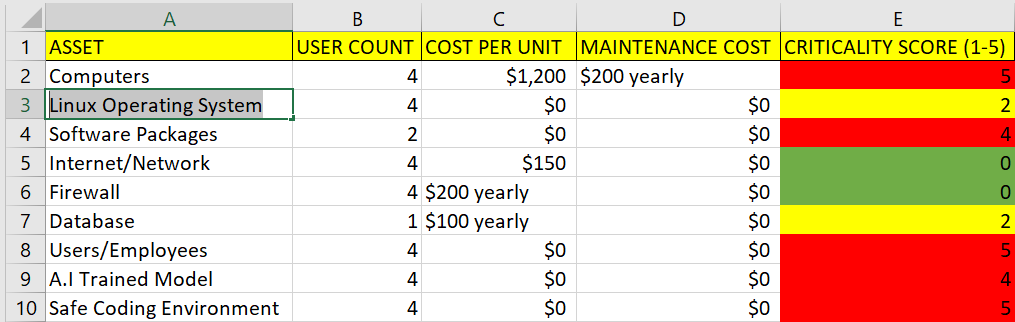
1. Presentation
2. Physical Report
3. Cyber Security Framework

Professional Accomplishments:

1. Learn what goes into a quality risk register and how to construct one properly
2. Have the ability to make a detailed SWOT analysis
3. Familiarity with NIST, CIS controls, and ISO/IEC
4. Become comfortable with working with security controls and how to use them proplerly
5. Working as a team cooperatively and understanding what works for each other

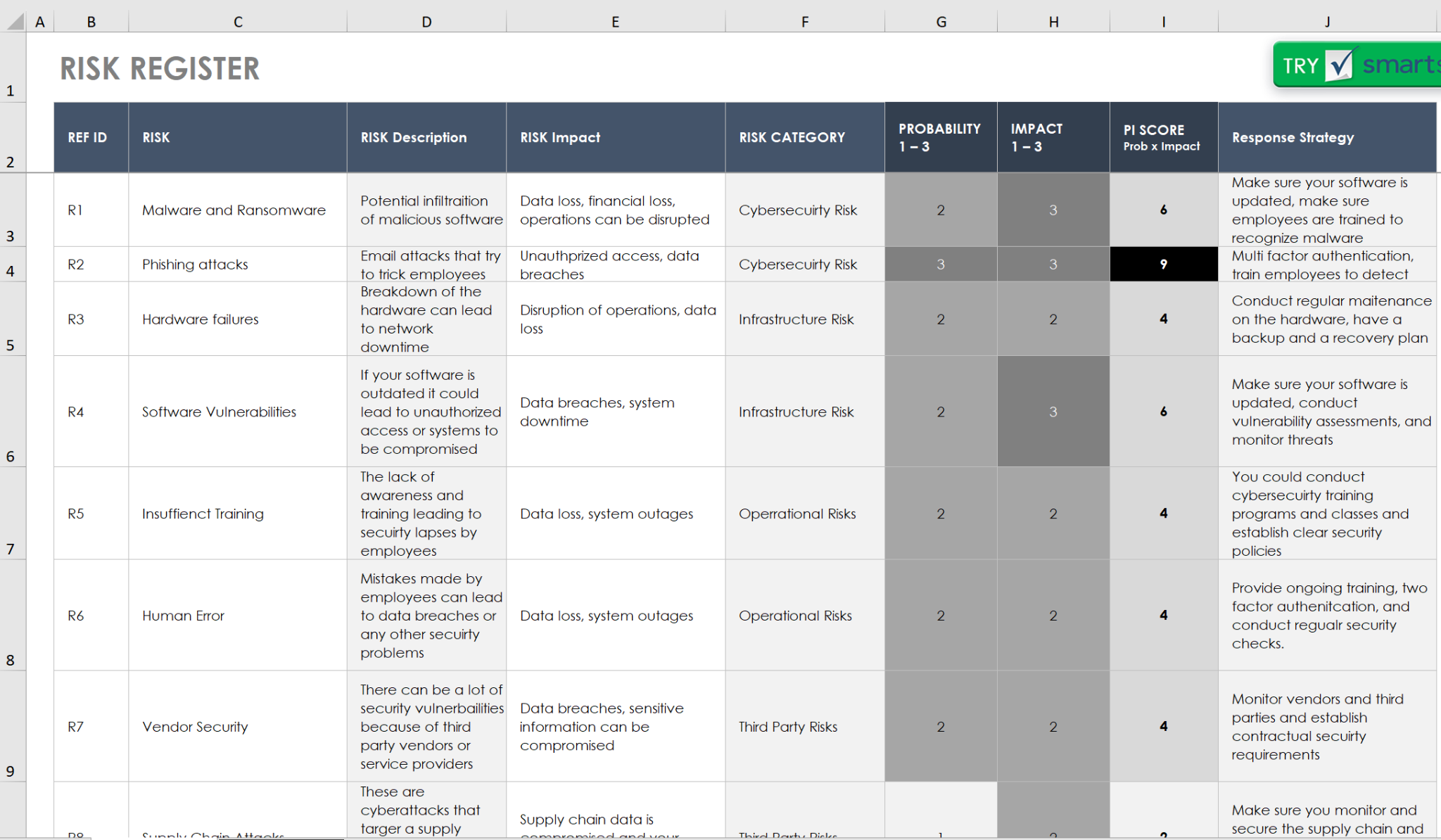
# Asset Inventory

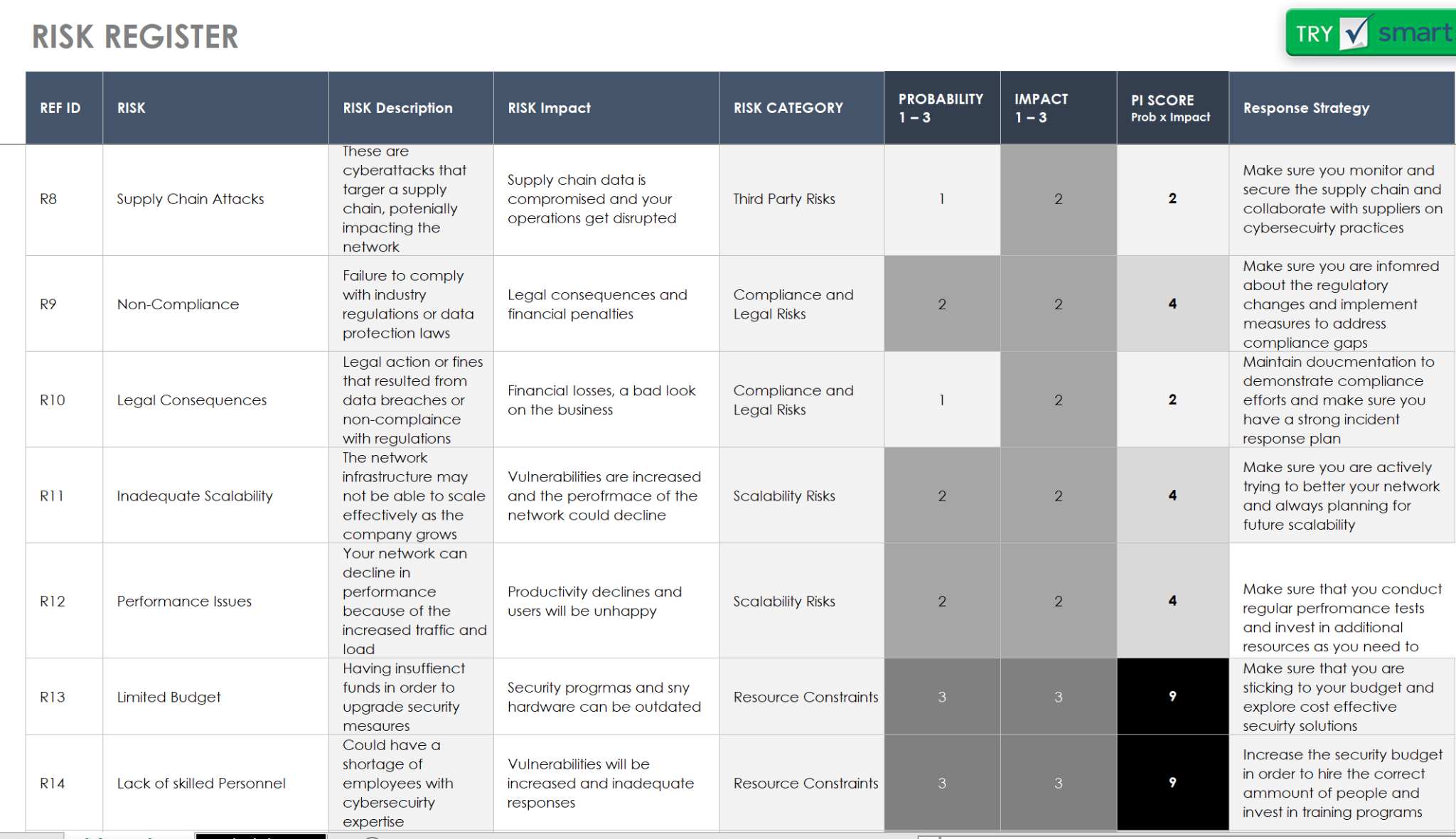
The start of Cyber Security at any organization. Without a list of assets, there is no way to secure the risks that can occur because there is no telling what area of the network that can be affected. If the organization does not have an asset inventory that is kept up to date, then a new asset inventory should be created, first starting with a network scanner. This asset inventory will be the baseline for the risk and vulnerability assessments and will provide guidance throughout the security process as the organization develops and implements their own cyber security framework. Our organization started by listing the assets that were known to be used and whatever was found during assessment. Our organization also added monetary cost and a criticality score for each of the assets.



Criticality score is reached by: (Frequency of attacks in a year 0-3) + (How much it will affect the organization 0-3)

# Risk Register

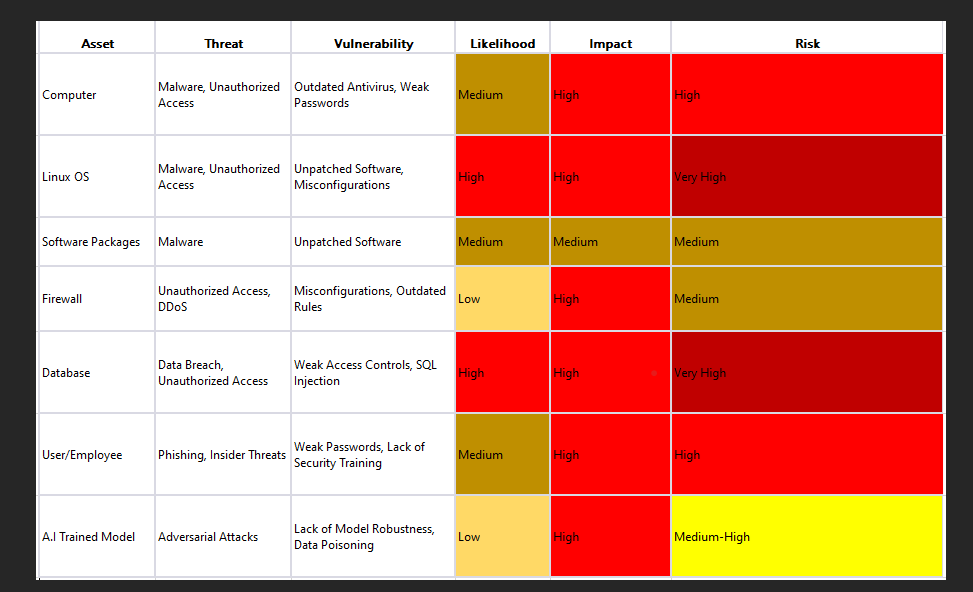






The risk register for this network shows the several crirtical cybersecurity risks, infrastructure risks, operational risks, third party risks, compliance and legal risks, scalability risks, resource constraints, incident response risks, regulatory changes, and social engineering risks that would negatively affect the network and would require immediate attenion. Each category has two risks that we identified and they each have their own level of likelihood of happening and level of impact. Each risk has their own solution of being fixed if the risk does end up happening. The best way to prevent these risks from happening is to be cautious of everything around you and to always be willing and ready to adapt.

# Risk Assessment

Once assets are defined, the organization needs to take steps in finding areas where risk is prevalent, and document the outcomes if those risks were to be fully realized is a process of evaluating potential risks to an organization or system, analyzing their impact and likelihood, and prioritizing them based on their significance. In the context of cybersecurity, risk assessment helps organizations understand the threats they face, the vulnerabilities in their systems, and the potential impact of these threats exploiting those vulnerabilities. Here is an example of our own Vulnerability-Based Risk assessment. 

# Secure Controls Framework

Once the risks are fully explored to each asset of the organization, implementation of controls where necessary is the next step in securing the company network. There are 33 Principles of SCF. This catalog of controls provides guidance to enable companies to design, build, maintain secure processes, systems and applications. With controls, concerns in both cybersecurity and privacy are addressed. It is highly recommended to look at the Secure Controls Framework (SCF), in doing so it will assist with the securing of confidentiality, integrity and availability (C.I.A triad) in security systems.







# Vulnerability Assessment

Once the controls are in place and optimized for the organization, the organization needs to scan and find where their network could be exploited.

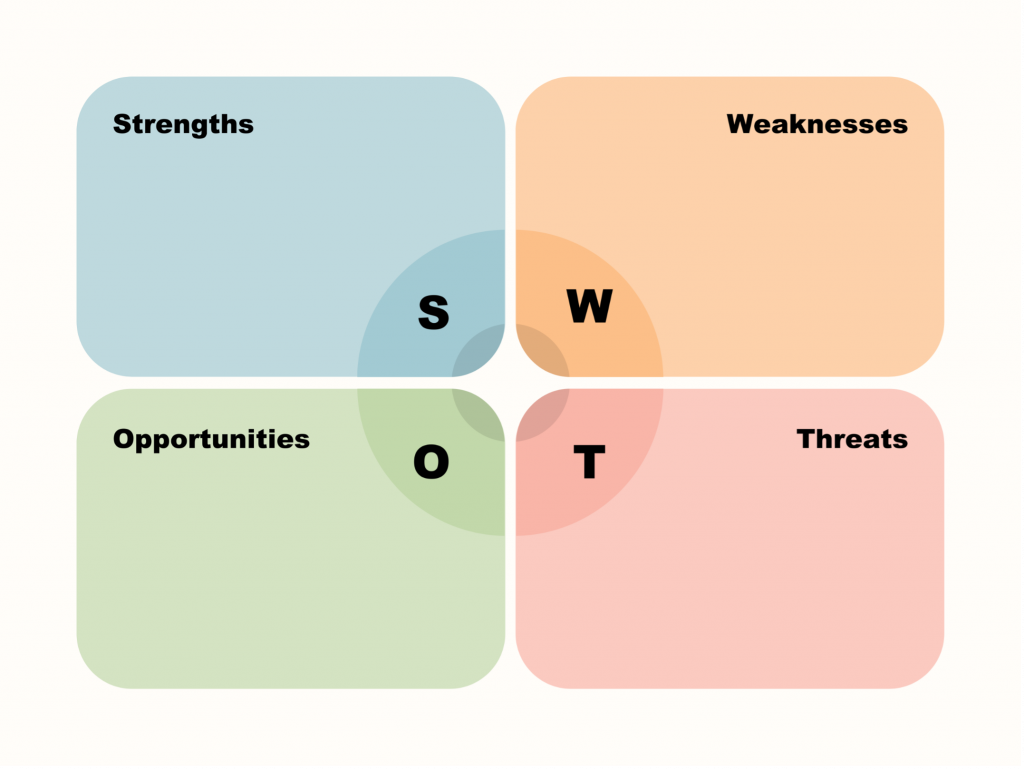


This is our detailed Vulnerability Assessment that outlines the findings and results of a systematic evaluation of the security vulnerabilities present in our system, network, application, or infrastructure. The primary purpose of a Vulnerability Assessment is to identify weaknesses that could be exploited by attackers to compromise the confidentiality, integrity, or availability of the target, we used the Host-based scans methodology.

# 

# SWOT Analysis

A SWOT analysis is recommended to take a step back and look at the organization as a whole in regards to business and security. This will help define the strengths, weaknesses, opportunities, and threats that the org faces in order to define plans to build on security with business profits in mind.



In our network here is how our SWOT analysis would look:

**Strengths**

* Cost effective security
* Scalability
* Security frameworks
* Access control

**Weaknesses**

* Limited budget
* Resources could be slightly older and not as effective
* The older hardware could have a lot of vulnerabilities due to due to the non updated systems
* Limited number of security members in the company

**Opportunities**

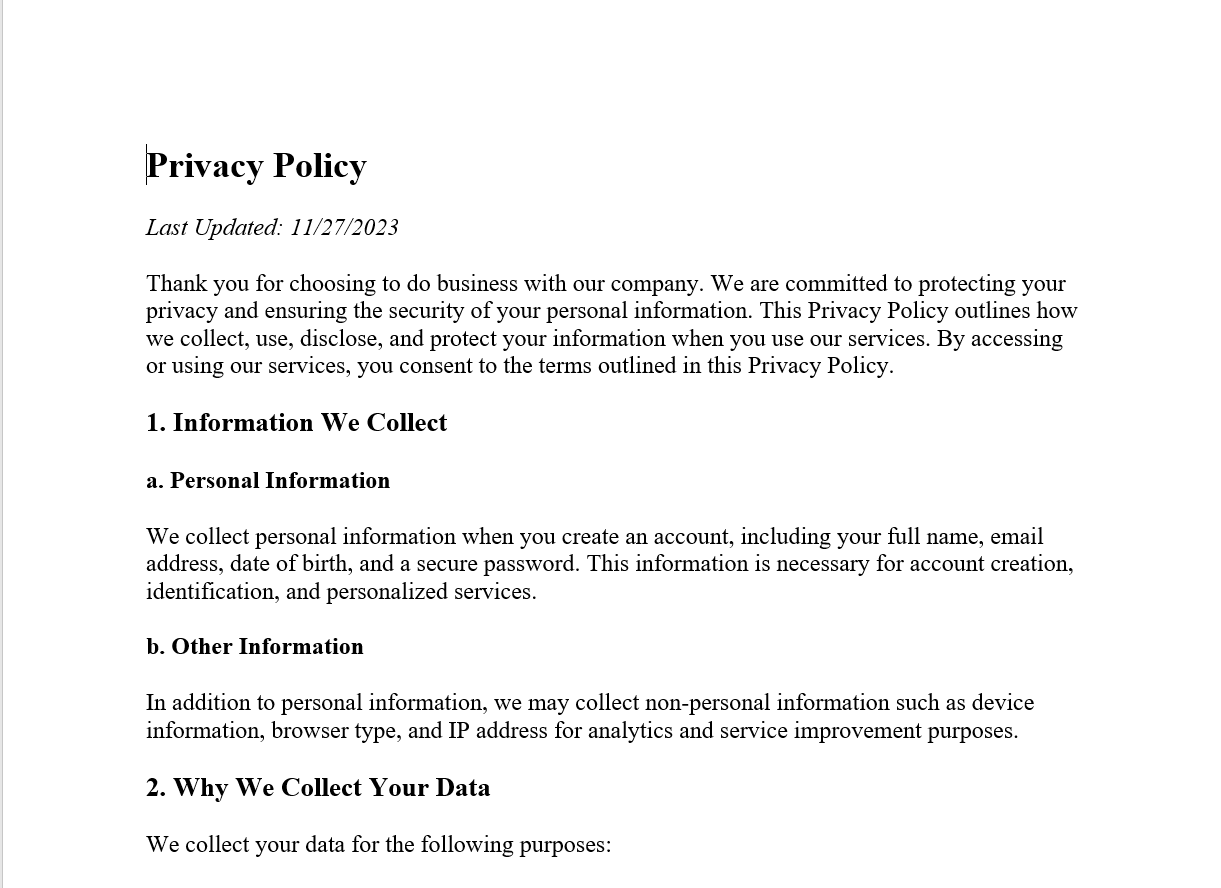
* Company could offer cyber classes and courses to better their employees
* The business growth can add to the budget of of security measures and resources

**Threats**

* Cyber attacks such as phishing, malware attacks, viruses, etc
* Third party risks
* Social engineering attacks
* User error

# GRC

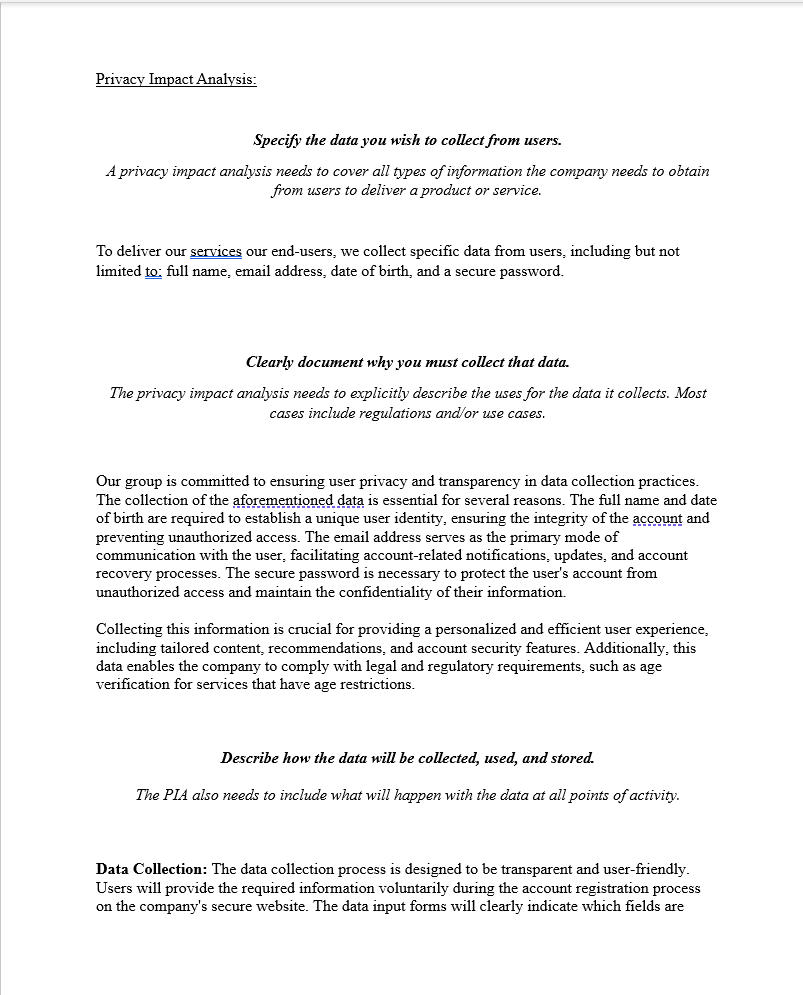
(GRC): Governance, Risk and Compliance is critical for setting up the security culture in the organization. Organizations are far more secure when all aspects of the company talk about and assess security measures, even at the top level. GRC is used to ensure that the company and employees do not become a high risk to the business’ operations whether it is legal, risk, or malicious behavior. GRC is used as a way to define what someone should do and how they should do it according to the law or policy set by the company. Our organization made policies that reflect our own cybersecurity mission that also aligns with standards set by NIST or legal requirements. GRC needs to be looked at from an inside perspective of the organization and an outside perspective (users/customers) in order to cover all areas of governance, risk, and compliance. This can be assisted by analyzing the risk register or asset inventory and looking for what type of data you will be handling through a privacy impact analysis or a business impact analysis explained later in the report.



# Cyber Hygiene

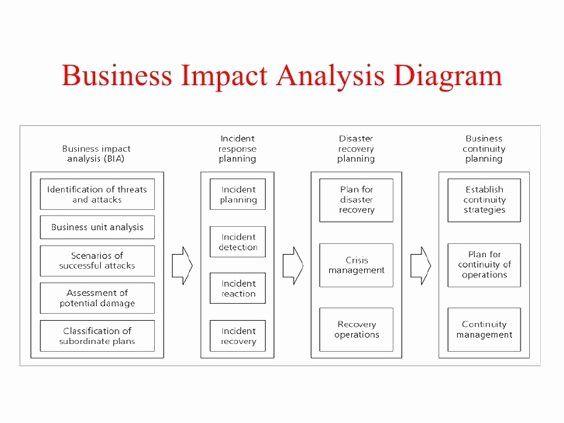
Cyber hygiene is the last part of implementing security at your own organization. Cyber hygiene refers to the overall Cyber Security environment surrounding the controls and practices in place. One thing that organizations can or should do is provide a privacy impact analysis. A privacy impact analysis describes the impact the organization will have on user data and can include other areas that are instead inside the organization. The data needs to be defined with: what is being collected, why must the data be collected, how it will be collected, the risks of collecting the data, and the measures the organization will take to mitigate those risks. All of these points of documentation are important for realizing the possible risk areas for handling data and upholding a good cyber hygiene.

**Privacy Impact Analysis (PIA)**

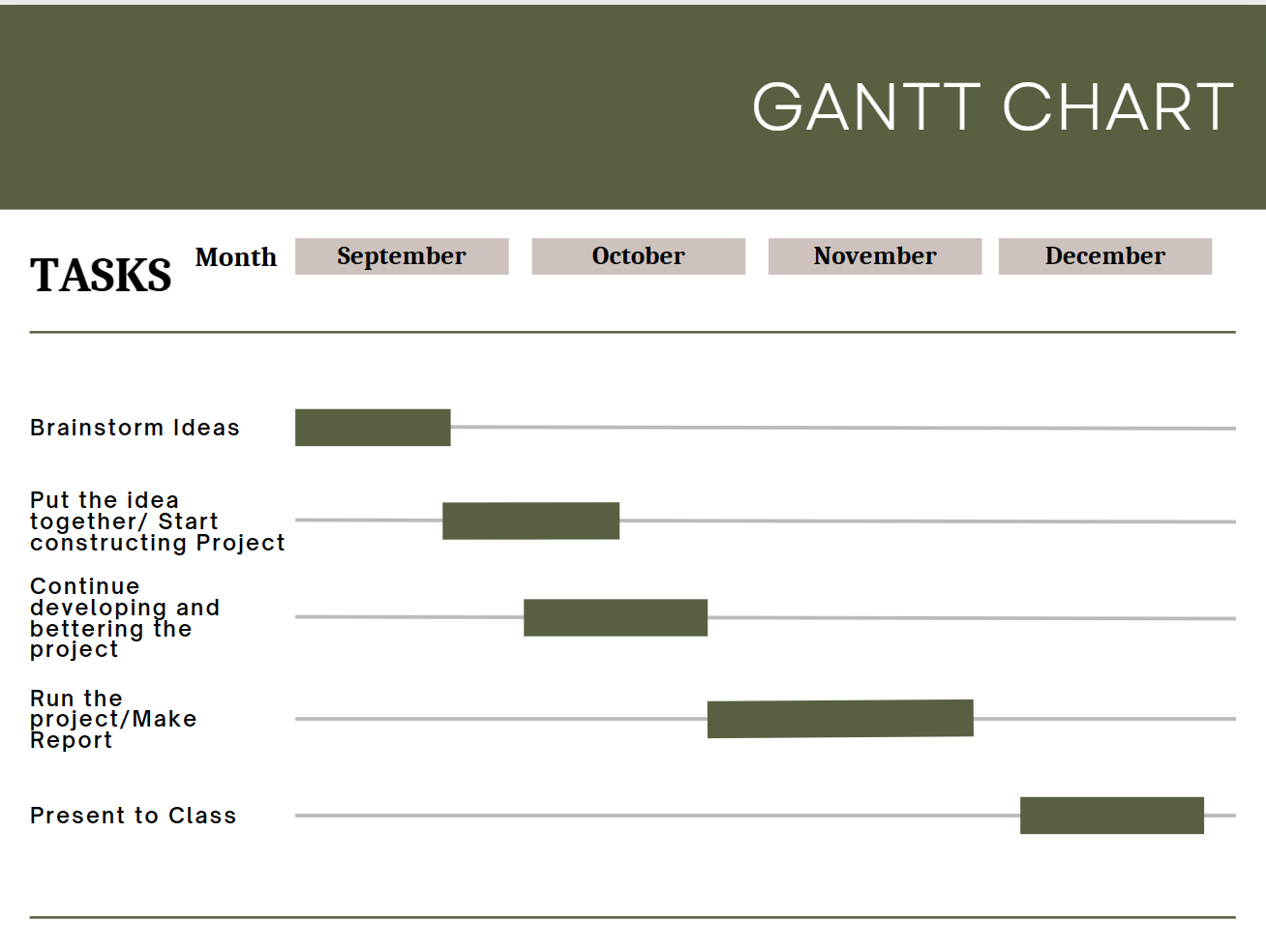


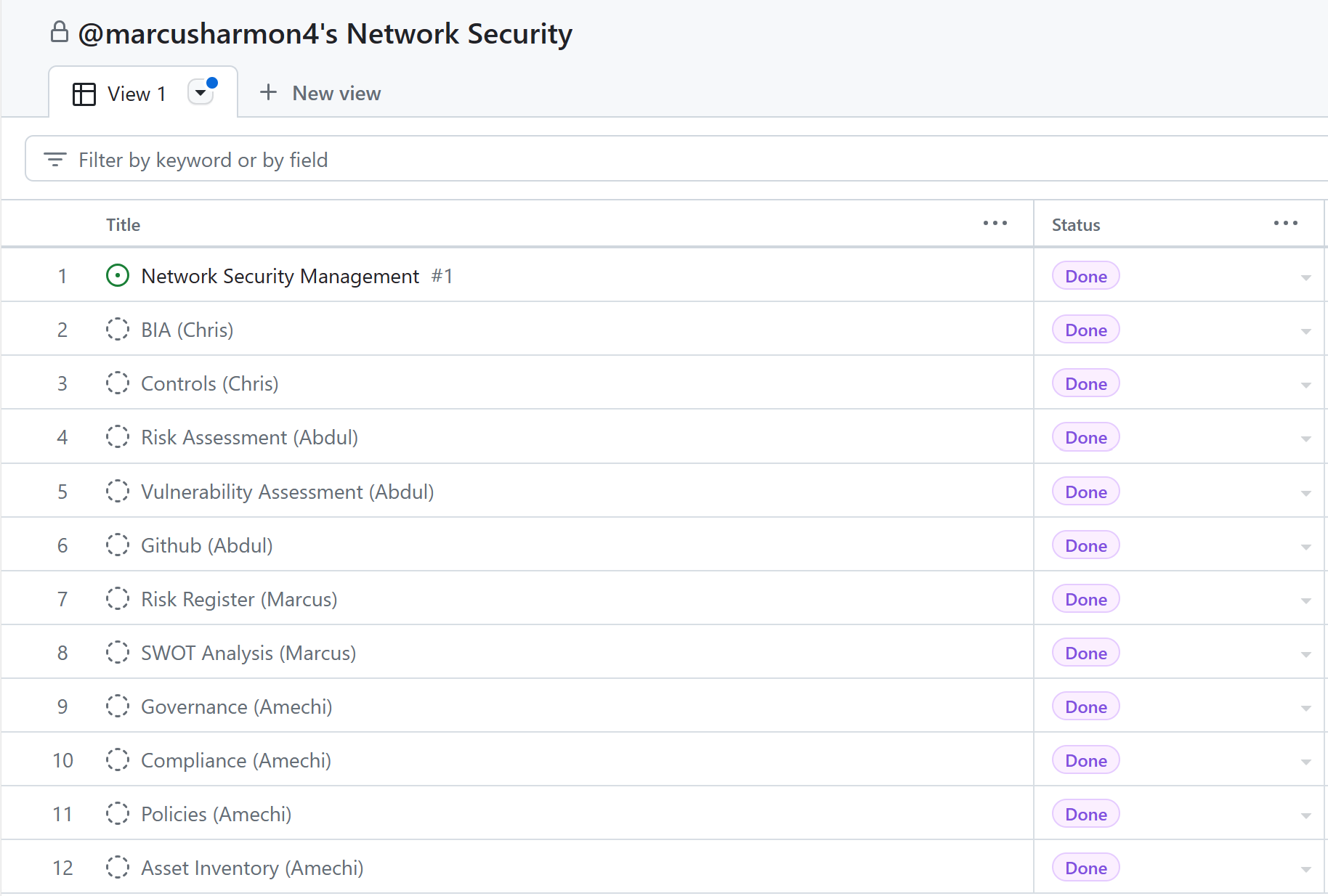
# Business Impact Analysis (BIA)

A dedicated BIA allows an organization to prepare for the worst to happen as the company can rebuild or continue business operations with as little disruption to happen as possible. By proactively reviewing risks and their impact in the risk register, an entity can develop a strong BIA plan that ensures the continuity of business.



# PROJECT SCHEDULE MANAGEMENT





GitHub Link: https://github.com/alqarni360/Security-Management-class

**Conclusion**

In today’s business landscape for low to middle end compnaines having a network that is safe and secure, along with reliable frameworks is the key to having a successful business. Although the network does have it’s weaknesses such as the limited budget, older and less effective resources, and the limited number of security members in the company these can be fixed with the business growth which can then be added to the budget of security measures and resources, cyber classes and courses can be used to better the members as well, and simply constantly updating the hardware and software that is being used. The network itself does have threats such as cyberattacks and third party risks. The best way to neutralize these threats is by regularly updating your software, constantly monitoring your systems, and making sure your employees are aware of what they need to be doing in order to have a secure network. At the end of the day, when you're building a network for low to middle end companies it will be an everlasting process. One of the most important things you can do is work towards and with your strenghts, assess your weaknesses, learn how to take advantage of your opportunities, and limit your threats. As your company and technology involves so must your network. The key is to be adaptive and to always be ready for any alerts and or changes.

# References

Template Link for Risk Register: [Get started with your work account | Smartsheet](https://www.smartsheet.com/try-it?trp&utm_source=integrated+content&utm_campaign=/risk-register-templates&utm_medium=risk+register+9419&lpa=risk+register+9419&lx=uE-y-RrkBugadNhJEVDq4l2F3tjZfBYMXSEruozjq1E)

National Cyber Security Centre- <https://www.ncsc.gov.uk/blog-post/ncsc-cyber-security-training-for-staff-now-available>

Link for Business Analysis Impact: https://www.allformtemplates.com/business-analysis-templates-15-free-analysis-sample-example-format/