Secure Architecture Report

By: Danielle Daza

TABLE OF CONTENTS

EXECUTIVE SUMMARY

Within this report, the NIST Cybersecurity Framework has been used as a template to customize to the organization needs and potential improvements. The NIST CSF is a risk-based framework of cybersecurity practices designed for the organizations to help manage and reduce cybersecurity risks. IT provides a structured approach to cybersecurity by aligning security activities with business and mission requirements. The primary functions this report will focus on will be Govern (GV) Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC). However, given the size of the organization, Govern (GV) is a function with the NIST CSF that is a supplementary consideration to the recommendations made in order to better focus on the fundamentals of cybersecurity architecture that appears to lacking and therefore deemed to be of higher priority.

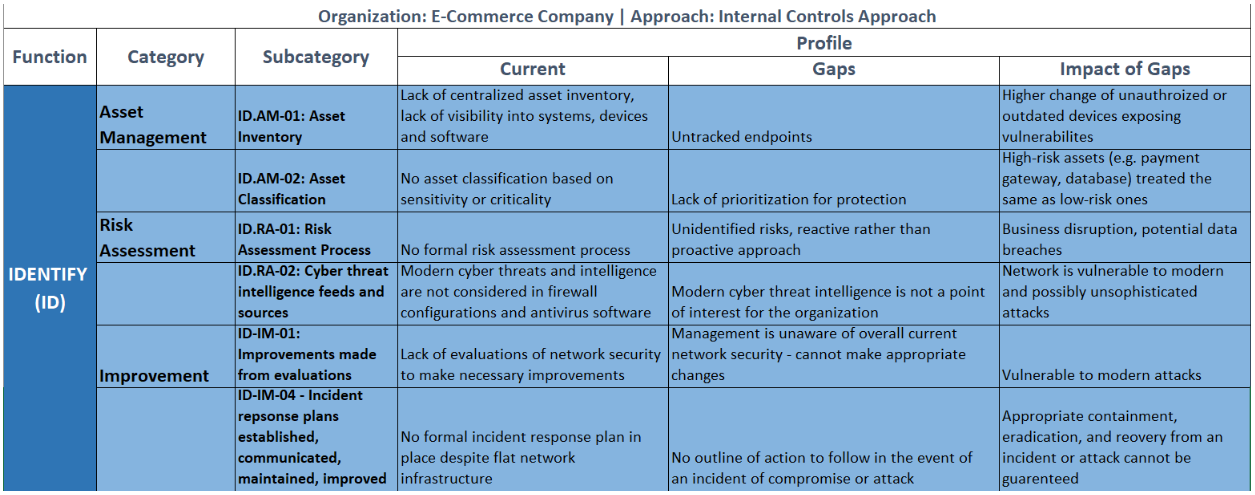
From the current state of the security, it is clear that substantial changes to the foundations need to be made in order to develop a more practical network in the modern threat landscape. From the analysis conducted, it was observed that several gaps in data security are principally due to the single physical server reliance, lack of network segmentation of the public-facing and internal operations, and the lack of modern security measure standards (e.g. monitoring practices, incident response and contingency planning, backup strategy patch management) which creates an environment conducive to various associating vulnerabilities within the infrastructure. As such, a roadmap of necessary tasks required to address these vulnerabilities have been developed and customized to the medium-sized the organization. The roadmap provided is divided by priority to best attain the target security profile in a logistical yet holistic way. Critical tasks are recommended to complete within 3 months of this report, high priority tasks within 3-6 months, and medium priority tasks 6 months or more. Additionally, designated responsibility owners and scalability considerations have been incorporated to ensure that security enhancements align with the organization’s size, budget, and long-term growth objectives.

SECURITY ARCHITECTURE ASSESSMENT

This section will cover the assessment of both the current profile of the organization. The primary functions of the NIST CSF referenced in the tables found in this section are Identify (ID), Protect (PR), Detect (DE), Respond (RS), and Recover (RC) – withholding the first function in stipulated in the framework, Govern (GV). Given the current state and size of the security architecture, the focus of this report and its recommendations is the essentials of a strong data security over the governance aspect of cybersecurity. It was deemed reasonable to address the primary points of concern in the overall infrastructure first with a secondary focus on implementing the necessary formal oversight and policies.

CURRENT PROFILE

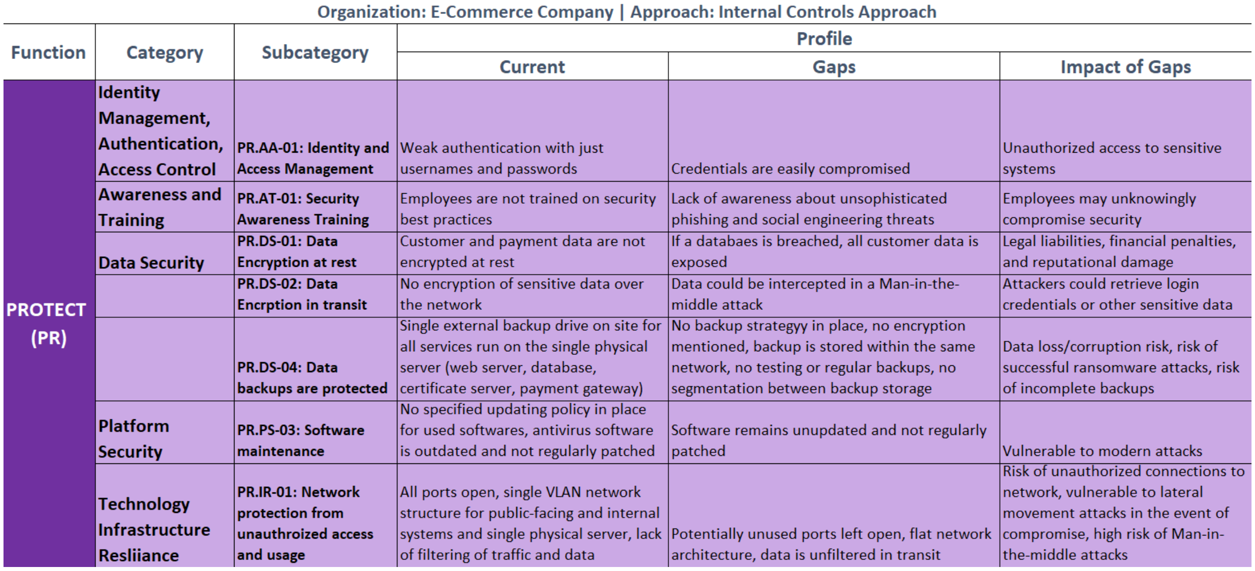
Below is an assessment of the current security architecture using the NIST CSF v2 as a reference with the intention of establishing a pragmatic yet solid groundwork for a medium-sized the organization. Within the table, the NIST primary function, relevant category and subcategory are presented with an analysis of the current profile outlined along with the gaps and its impact discovered in relation to the subcategory of the security function. The categories and subcategories were chosen as most essential security measures required for the size and budget of the organization.



Organization: E-Commerce Company | Approach: Internal Controls Approach

Function	Category	Subcategory	Profile		
			Current	Gaps	Impact of Gaps
IDENTIFY (ID)	Asset Management	ID.AM-01: Asset Inventory	Lack of centralized asset inventory, lack of visibility into systems, devices and software	Untracked endpoints	Higher change of unauthroized or outdated devices exposing vulnerabilites
		ID.AM-02: Asset Classification	No asset classification based on sensitivity or criticality	Lack of prioritization for protection	High-risk assets (e.g. payment gateway, database) treated the same as low-risk ones
	Risk Assessment	ID.RA-01: Risk Assessment Process	No formal risk assessment process	Unidentified risks, reactive rather than proactive approach	Business disruption, potential data breaches
		ID.RA-02: Cyber threat intelligence feeds and sources	Modern cyber threats and intelligence are not considered in firewall configurations and antivirus software	Modern cyber threat intelligence is not a point of interest for the organization	Network is vulnerable to modern and possibly unsophisticated attacks
	Improvement	ID-IM-01: Improvements made from evaluations	Lack of evaluations of network security to make necessary improvements	Management is unaware of overall current network security - cannot make appropriate changes	Vulnerable to modern attacks
		ID-IM-04 - Incident repsonse plans established, communicated, maintained, improved	No formal incident response plan in place despite flat network infrastructure	No outline of action to follow in the event of an incident of compromise or attack	Appropriate containment, eradication, and reovery from an incident or attack cannot be guarenteed

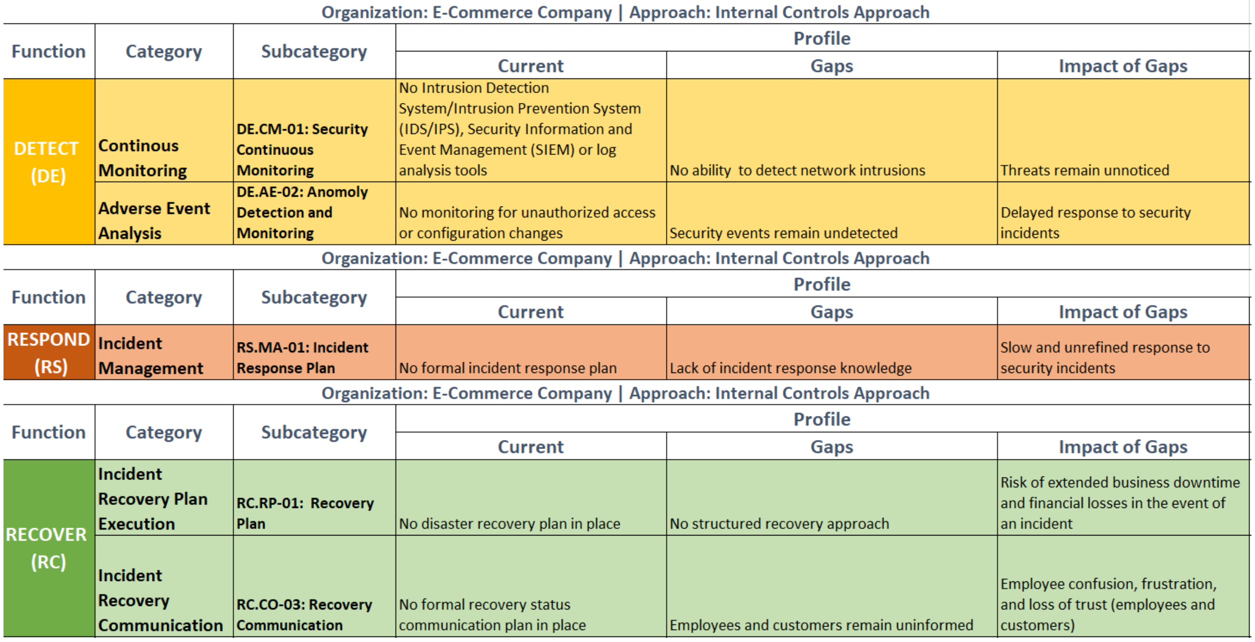
Figure 1.1 – Identify function of current profile using NIST CSF v2.



Organization: E-Commerce Company | Approach: Internal Controls Approach

Function	Category	Subcategory	Profile		
			Current	Gaps	Impact of Gaps
PROTECT (PR)	Identity Management, Authentication, Access Control	PR.AA-01: Identity and Access Management	Weak authentication with just usernames and passwords	Credentials are easily compromised	Unauthorized access to sensitive systems
	Awareness and Training	PR.AT-01: Security Awareness Training	Employees are not trained on security best practices	Lack of awareness about unsophisticated phishing and social engineering threats	Employees may unknowingly compromise security
	Data Security	PR.DS-01: Data Encryption at rest	Customer and payment data are not encrypted at rest	If a databaes is breached, all customer data is exposed	Legal liabilities, financial penalties, and reputational damage
		PR.DS-02: Data Encrption in transit	No encryption of sensitive data over the network	Data could be intercepted in a Man-in-the-middle attack	Attackers could retrieve login credentials or other sensitive data
		PR.DS-04: Data backups are protected	Single external backup drive on site for all services run on the single physical server (web server, database, certificate server, payment gateway)	No backup strategyy in place, no encryption mentioned, backup is stored within the same network, no testing or regular backups, no segmentation between backup storage	Data loss/corruption risk, risk of successful ransomware attacks, risk of incomplete backups
	Platform Security	PR.PS-03: Software maintenance	No specified updating policy in place for used softwares, antivirus software is outdated and not regularly patched	Software remains unupdated and not regularly patched	Vulnerable to modern attacks
	Technology Infrastructure Resliiance	PR.IR-01: Network protection from unauthroized access and usage	All ports open, single VLAN network structure for public-facing and internal systems and single physical server, lack of filtering of traffic and data	Potentially unused ports left open, flat network architecture, data is unfiltered in transit	Risk of unauthorized connections to network, vulnerable to lateral movement attacks in the event of compromise, high risk of Man-in-the-middle attacks

Figure 1.2 – Protect function of current profile using NIST CSF v2.



Organization: E-Commerce Company | Approach: Internal Controls Approach

Function	Category	Subcategory	Profile		
			Current	Gaps	Impact of Gaps
DETECT (DE)	Continous Monitoring	DE.CM-01: Security Continuous Monitoring	No Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Security Information and Event Management (SIEM) or log analysis tools	No ability to detect network intrusions	Threats remain unnoticed
	Adverse Event Analysis	DE.AE-02: Anomoly Detection and Monitoring	No monitoring for unauthorized access or configuration changes	Security events remain undetected	Delayed response to security incidents

Organization: E-Commerce Company | Approach: Internal Controls Approach

Function	Category	Subcategory	Profile		
			Current	Gaps	Impact of Gaps
RESPOND (RS)	Incident Management	RS.MA-01: Incident Response Plan	No formal incident response plan	Lack of incident response knowledge	Slow and unrefined response to security incidents

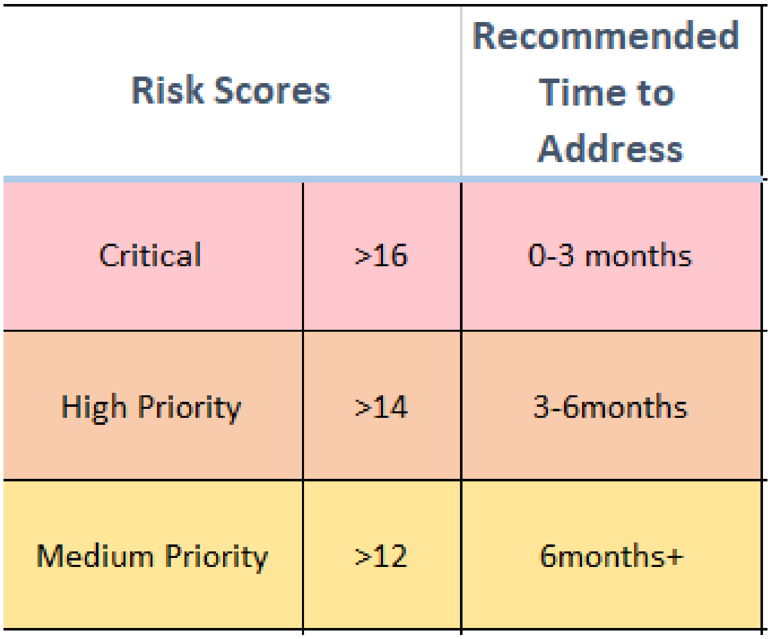
Organization: E-Commerce Company | Approach: Internal Controls Approach

Function	Category	Subcategory	Profile		
			Current	Gaps	Impact of Gaps
RECOVER (RC)	Incident Recovery Plan Execution	RC.RP-01: Recovery Plan	No disaster recovery plan in place	No structured recovery approach	Risk of extended business downtime and financial losses in the event of an incident
	Incident Recovery Communication	RC.CO-03: Recovery Communication	No formal recovery status communication plan in place	Employees and customers remain uninformed	Employee confusion, frustration, and loss of trust (employees and customers)

Figure 1.3 – Detect, Respond and Recover function of current profile using NIST CSF v2.

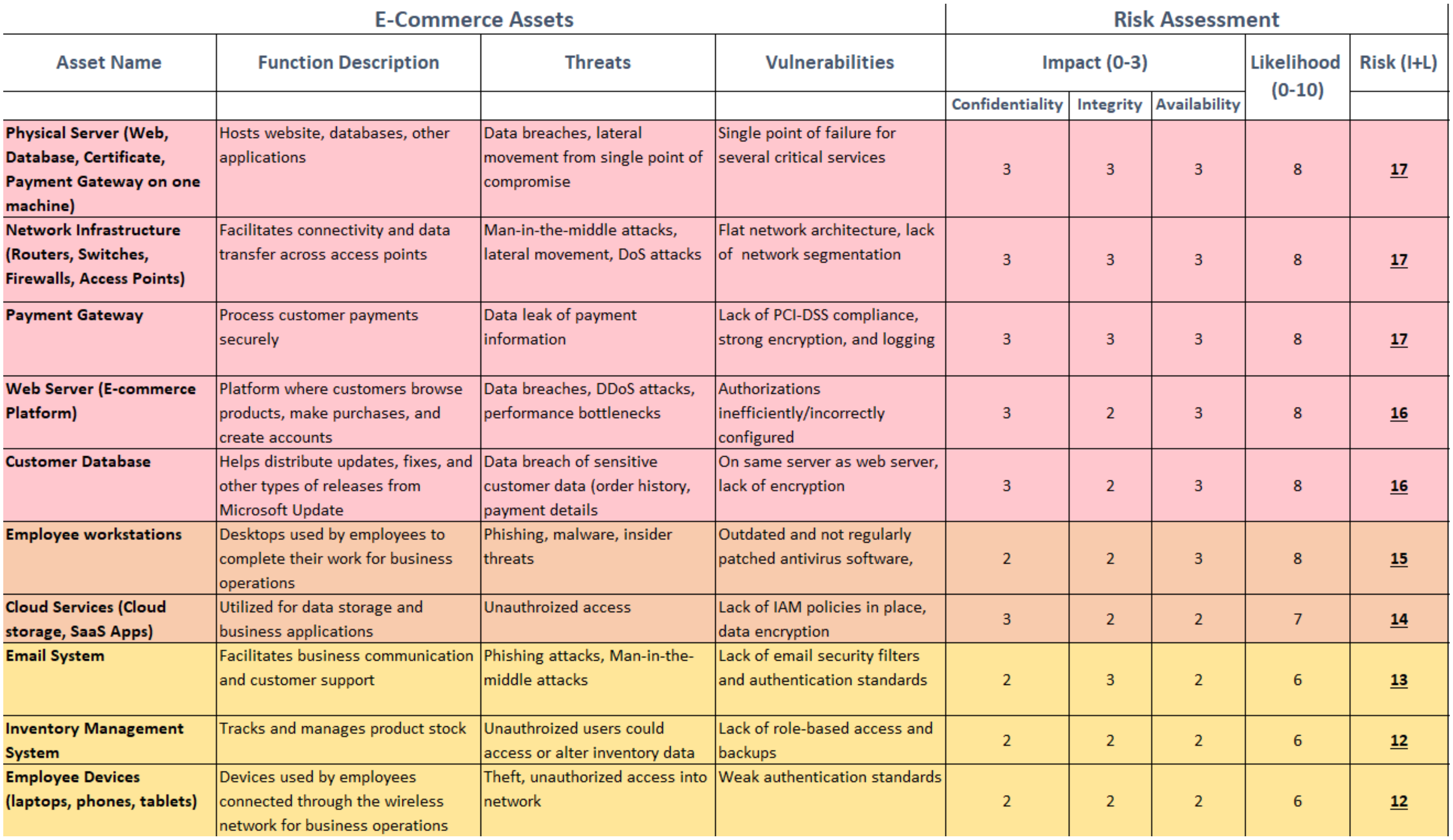
As seen in Figure 1.1, heavy emphasis on the Identify (ID) and Protect (PR) functions are of most concern in the organization's current cybersecurity state. This is largely due to the single physical server reliance, lack of network segmentation of the public-facing and internal operations, and the general lack of modern security measure standards (e.g. modern encryption, backup strategy, update and patch management, monitoring practices) which feed into various other vulnerabilities and gaps within the infrastructure. In addition, a significant oversight on contingency planning was also observed when analyzing the organization's structural outline. As such, a recommended target profile and the necessary actions required will be outlined in an expanded table in a later section of this report.

With the analysis of the current profile and the assets of The organization detailed, a supplementary analysis was conducted on the risks observed in the current network. Below is a risk assessment done on the assets of The organization in order of importance to the organization as well as a legend to the table. The risks' impacts were determined with the reference of the CIA triad – confidentiality (limiting data access), integrity (ensuring accurate data), and availability (data is consistently and readily accessible for authorized parties) (Hashemi-PourCameron, 2023).



Risk Scores		Recommended Time to Address
Critical	>16	0-3 months
High Priority	>14	3-6months
Medium Priority	>12	6months+

Figure 2.5 – Risk Assessment legend for reference.



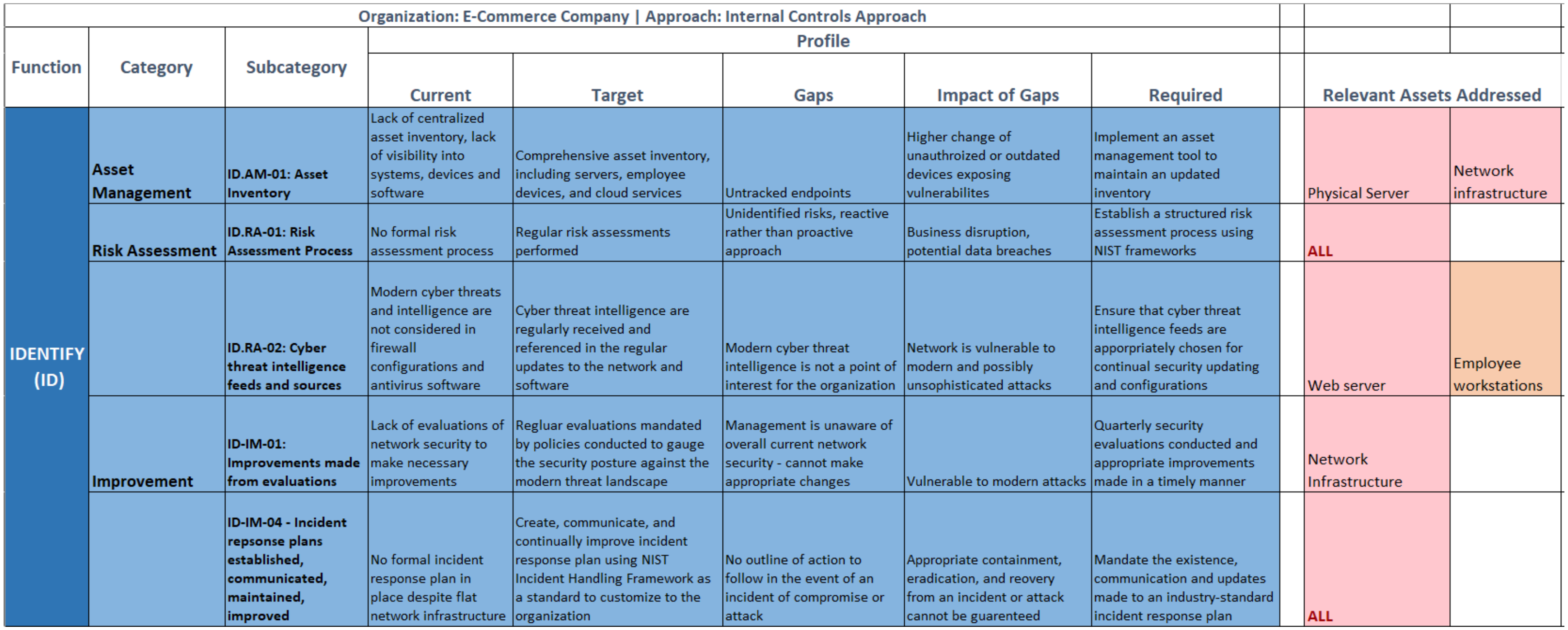
E-Commerce Assets				Risk Assessment				
Asset Name	Function Description	Threats	Vulnerabilities	Impact (0-3)			Likelihood (0-10)	Risk (I+L)
				Confidentiality	Integrity	Availability		
Physical Server (Web, Database, Certificate, Payment Gateway on one machine)	Hosts website, databases, other applications	Data breaches, lateral movement from single point of compromise	Single point of failure for several critical services	3	3	3	8	**17**
Network Infrastructure (Routers, Switches, Firewalls, Access Points)	Facilitates connectivity and data transfer across access points	Man-in-the-middle attacks, lateral movement, DoS attacks	Flat network architecture, lack of network segmentation	3	3	3	8	**17**
Payment Gateway	Process customer payments securely	Data leak of payment information	Lack of PCI-DSS compliance, strong encryption, and logging	3	3	3	8	**17**
Web Server (E-commerce Platform)	Platform where customers browse products, make purchases, and create accounts	Data breaches, DDoS attacks, performance bottlenecks	Authorizations inefficiently/incorrectly configured	3	2	3	8	**16**
Customer Database	Helps distribute updates, fixes, and other types of releases from Microsoft Update	Data breach of sensitive customer data (order history, payment details	On same server as web server, lack of encryption	3	2	3	8	**16**
Employee workstations	Desktops used by employees to complete their work for business operations	Phishing, malware, insider threats	Outdated and not regularly patched antivirus software,	2	2	3	8	**15**
Cloud Services (Cloud storage, SaaS Apps)	Utilized for data storage and business applications	Unauthroized access	Lack of IAM policies in place, data encryption	3	2	2	7	**14**
Email System	Facilitates business communication and customer support	Phishing attacks, Man-in-the-middle attacks	Lack of email security filters and authentication standards	2	3	2	6	**13**
Inventory Management System	Tracks and manages product stock	Unauthroized users could access or alter inventory data	Lack of role-based access and backups	2	2	2	6	**12**
Employee Devices (laptops, phones, tablets)	Devices used by employees connected through the wireless network for business operations	Theft, unauthorized access into network	Weak authentication standards	2	2	2	6	**12**

Figure 2.2 – Risk Assessment of E-Commerce assets.

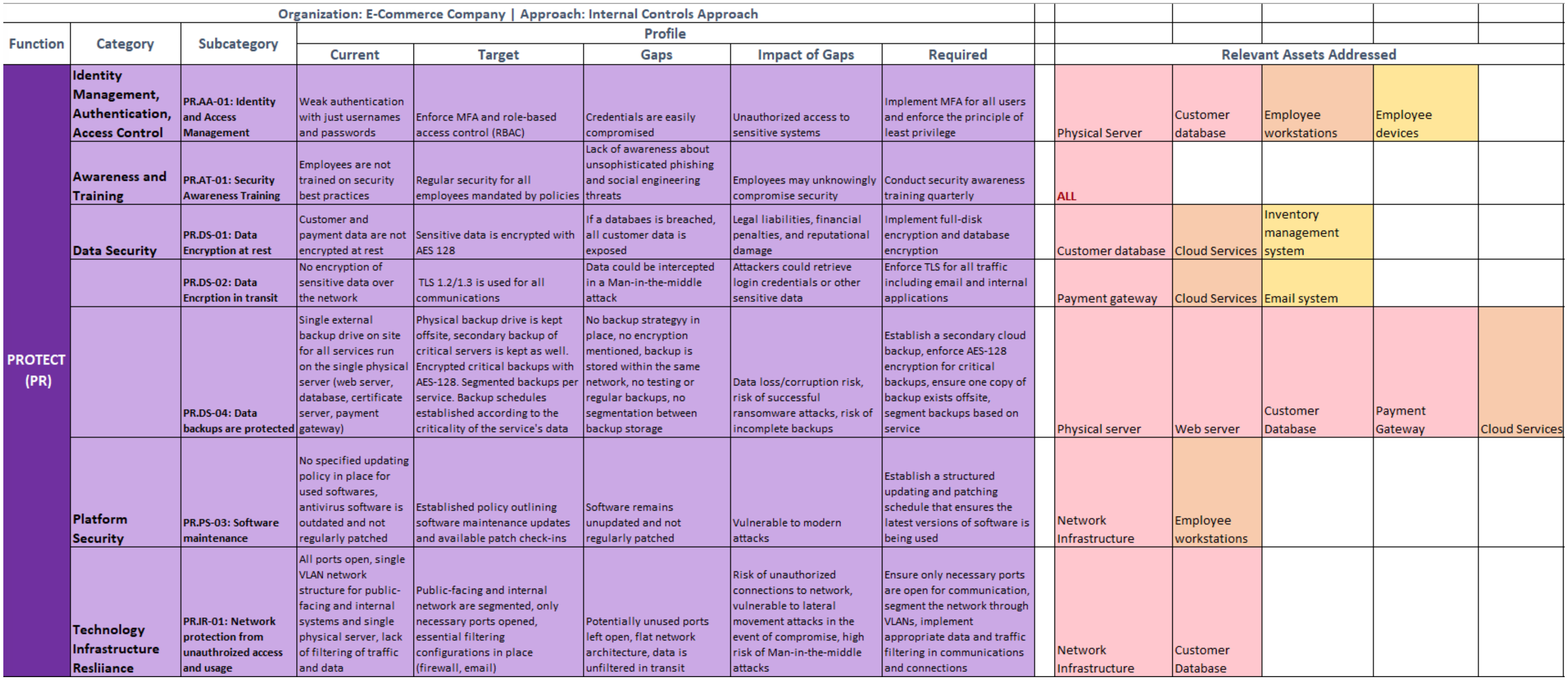
As evident in Figure 2.2, crucial services such as the physical server, the infrastructure itself, and the payment gateway for customers are of critical importance as the impacts of the relevant risks – referring to the CIA triad – are quite severe given the current state of the network.

TARGET PROFILE

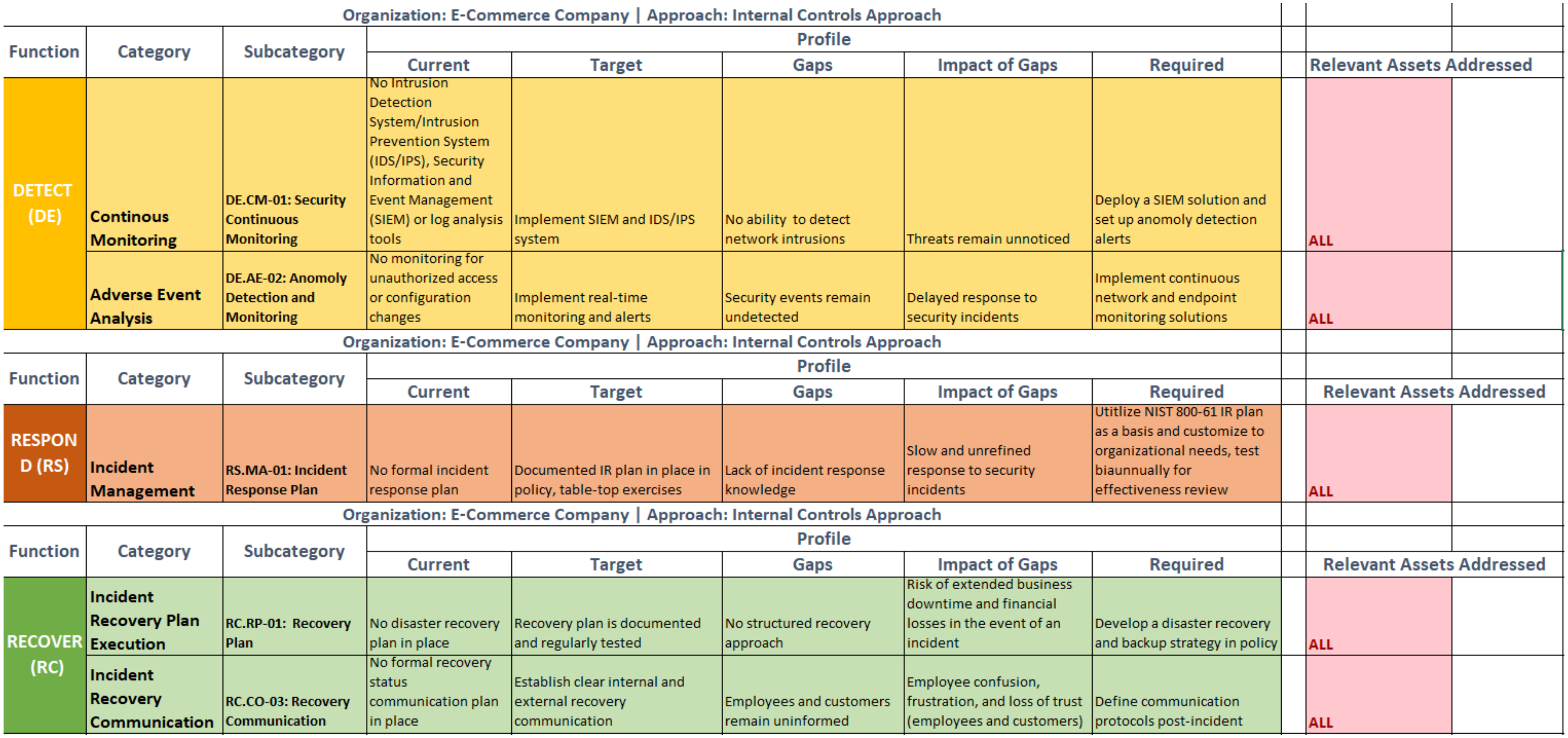
With the risk assessment of assets and the current profile and its gaps delineated, the recommended target profile was developed for a comprehensive comparative view of the current and target profiles with the additional consideration of the relevant assets that each NIST CSF subcategory addresses. The following two pages contain the full NIST CSF analysis, recommended target profile and relevant assets to consider.



Organization: E-Commerce Company | Approach: Internal Controls Approach										
Function	Category	Subcategory	Profile						Relevant Assets Addressed	
			Current	Target	Gaps	Impact of Gaps	Required			
IDENTIFY (ID)	Asset Management	ID.AM-01: Asset Inventory	Lack of centralized asset inventory, lack of visibility into systems, devices and software	Comprehensive asset inventory, including servers, employee devices, and cloud services	Untracked endpoints	Higher change of unauthroized or outdated devices exposing vulnerabilites	Implement an asset management tool to maintain an updated inventory		Physical Server	Network infrastructure
	Risk Assessment	ID.RA-01: Risk Assessment Process	No formal risk assessment process	Regular risk assessments performed	Unidentified risks, reactive rather than proactive approach	Business disruption, potential data breaches	Establish a structured risk assessment process using NIST frameworks		ALL	
		ID.RA-02: Cyber threat intelligence feeds and sources	Modern cyber threats and intelligence are not considered in firewall configurations and antivirus software	Cyber threat intelligence are regularly received and referenced in the regular updates to the network and software	Modern cyber threat intelligence is not a point of interest for the organization	Network is vulnerable to modern and possibly unsophisticated attacks	Ensure that cyber threat intelligence feeds are apporpriately chosen for continual security updating and configurations		Web server	Employee workstations
	Improvement	ID-IM-01: Improvements made from evaluations	Lack of evaluations of network security to make necessary improvements	Regluar evaluations mandated by policies conducted to gauge the security posture against the modern threat landscape	Management is unaware of overall current network security - cannot make appropriate changes	Vulnerable to modern attacks	Quarterly security evaluations conducted and appropriate improvements made in a timely manner		Network Infrastructure	
		ID-IM-04 - Incident repsonse plans established, communicated, maintained, improved	No formal incident response plan in place despite flat network infrastructure	Create, communicate, and continually improve incident response plan using NIST Incident Handling Framework as a standard to customize to the organization	No outline of action to follow in the event of an incident of compromise or attack	Appropriate containment, eradication, and reovery from an incident or attack cannot be guarenteed	Mandate the existence, communication and updates made to an industry-standard incident response plan		ALL	



Organization: E-Commerce Company | Approach: Internal Controls Approach														
Function	Category	Subcategory	Profile						Relevant Assets Addressed					
			Current	Target	Gaps	Impact of Gaps	Required							
PROTECT (PR)	Identity Management, Authentication, Access Control	PR.AA-01: Identity and Access Management	Weak authentication with just usernames and passwords	Enforce MFA and role-based access control (RBAC)	Credentials are easily compromised	Unauthorized access to sensitive systems	Implement MFA for all users and enforce the principle of least privilege		Physical Server	Customer database	Employee workstations	Employee devices	
	Awareness and Training	PR.AT-01: Security Awareness Training	Employees are not trained on security best practices	Regular security for all employees mandated by policies	Lack of awareness about unsophisticated phishing and social engineering threats	Employees may unknowingly compromise security	Conduct security awareness training quarterly		ALL				
	Data Security	PR.DS-01: Data Encryption at rest	Customer and payment data are not encrypted at rest	Sensitive data is encrypted with AES 128	If a databaes is breached, all customer data is exposed	Legal liabilities, financial penalties, and reputational damage	Implement full-disk encryption and database encryption		Customer database	Cloud Services	Inventory management system		
		PR.DS-02: Data Encrption in transit	No encryption of sensitive data over the network	TLS 1.2/1.3 is used for all communications	Data could be intercepted in a Man-in-the-middle attack	Attackers could retrieve login credentials or other sensitive data	Enforce TLS for all traffic including email and internal applications		Payment gateway	Cloud Services	Email system		
		PR.DS-04: Data backups are protected	Single external backup drive on site for all services run on the single physical server (web server, database, certificate server, payment gateway)	Physical backup drive is kept offsite, secondary backup of critical servers is kept as well. Encrypted critical backups with AES-128. Segmented backups per service. Backup schedules established according to the criticality of the service's data	No backup strategyy in place, no encryption mentioned, backup is stored within the same network, no testing or regular backups, no segmentation between backup storage	Data loss/corruption risk, risk of successful ransomware attacks, risk of incomplete backups	Establish a secondary cloud backup, enforce AES-128 encryption for critical backups, ensure one copy of backup exists offsite, segment backups based on service		Physical server	Web server	Customer Database	Payment Gateway	Cloud Services
	Platform Security	PR.PS-03: Software maintenance	No specified updating policy in place for used softwares, antivirus software is outdated and not regularly patched	Established policy outlining software maintenance updates and available patch check-ins	Software remains unupdated and not regularly patched	Vulnerable to modern attacks	Establish a structured updating and patching schedule that ensures the latest versions of software is being used		Network Infrastructure	Employee workstations			
	Technology Infrastructure Resliiance	PR.IR-01: Network protection from unauthroized access and usage	All ports open, single VLAN network structure for public-facing and internal systems and single physical server, lack of filtering of traffic and data	Public-facing and internal network are segmented, only necessary ports opened, essential filtering configurations in place (firewall, email)	Potentially unused ports left open, flat network architecture, data is unfiltered in transit	Risk of unauthorized connections to network, vulnerable to lateral movement attacks in the event of compromise, high risk of Man-in-the-middle attacks	Ensure only necessary ports are open for communication, segment the network through VLANs, implement appropriate data and traffic filtering in communications and connections		Network Infrastructure	Customer Database			



Organization: E-Commerce Company | Approach: Internal Controls Approach								
Function	Category	Subcategory	Profile					
			Current	Target	Gaps	Impact of Gaps	Required	Relevant Assets Addressed
DETECT (DE)	Continous Monitoring	DE.CM-01: Security Continuous Monitoring	No Intrusion Detection System/Intrusion Prevention System (IDS/IPS), Security Information and Event Management (SIEM) or log analysis tools	Implement SIEM and IDS/IPS system	No ability to detect network intrusions	Threats remain unnoticed	Deploy a SIEM solution and set up anomoly detection alerts	ALL
	Adverse Event Analysis	DE.AE-02: Anomoly Detection and Monitoring	No monitoring for unauthorized access or configuration changes	Implement real-time monitoring and alerts	Security events remain undetected	Delayed response to security incidents	Implement continuous network and endpoint monitoring solutions	ALL

Organization: E-Commerce Company | Approach: Internal Controls Approach								
Function	Category	Subcategory	Profile					
			Current	Target	Gaps	Impact of Gaps	Required	Relevant Assets Addressed
RESPON D (RS)	Incident Management	RS.MA-01: Incident Response Plan	No formal incident response plan	Documented IR plan in place in policy, table-top exercises	Lack of incident response knowledge	Slow and unrefined response to security incidents	Utitlize NIST 800-61 IR plan as a basis and customize to organizational needs, test biaunnually for effectiveness review	ALL

Organization: E-Commerce Company | Approach: Internal Controls Approach								
Function	Category	Subcategory	Profile					
			Current	Target	Gaps	Impact of Gaps	Required	Relevant Assets Addressed
RECOVER (RC)	Incident Recovery Plan Execution	RC.RP-01: Recovery Plan	No disaster recovery plan in place	Recovery plan is documented and regularly tested	No structured recovery approach	Risk of extended business downtime and financial losses in the event of an incident	Develop a disaster recovery and backup strategy in policy	ALL
	Incident Recovery Communication	RC.CO-03: Recovery Communication	No formal recovery status communication plan in place	Establish clear internal and external recovery communication	Employees and customers remain uninformed	Employee confusion, frustration, and loss of trust (employees and customers)	Define communication protocols post-incident	ALL

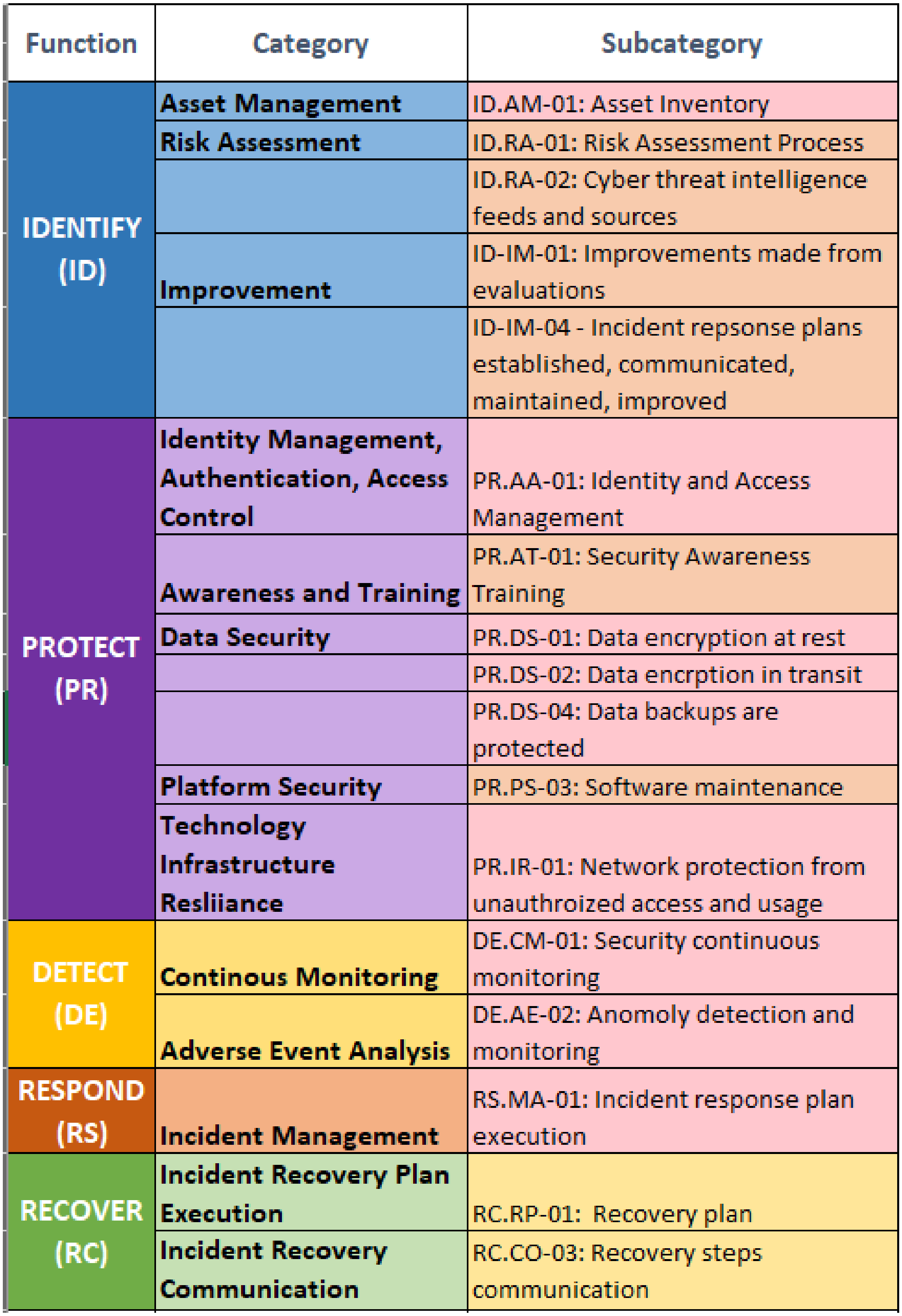
As evident from the analysis charts, there are a number of required actions being suggested in order to establish and maintain a strong security architecture. As such,

IMPLEMENTATION STRATEGY OF RECOMMENDATIONS

This section aims to provide guidance on the logistics of addressing the vulnerabilities and gaps that exist in the current the organization security infrastructure. As there are a number of critical tasks needed to address, the priorities of such tasks have been organized for a more structured and logical approach to the order of achieving the tasks. As outlined in the risk assessment, critical priority tasks are recommended to take 0-3 months to achieve or at least begin (dependent on potential budgetary or time limitations that may occur), high priority tasks are recommended to be completed within 3-6 months, and medium priority tasks are recommended to take 6 or more months to complete as they are still of concern but not in need of immediate attention. Within each priority heading will be the primary objective that the tasks within that heading aim to achieve.

TASKS TO ADDRESS

Below is a summary of the tasks that the timeline sections will address. The colours of the subcategory cells indicate the priority. Though several are under the "critical" priority, there are overlapping tasks regarding that subcategory in the high or medium priority as some subcategories entail a more layered approach to achieving

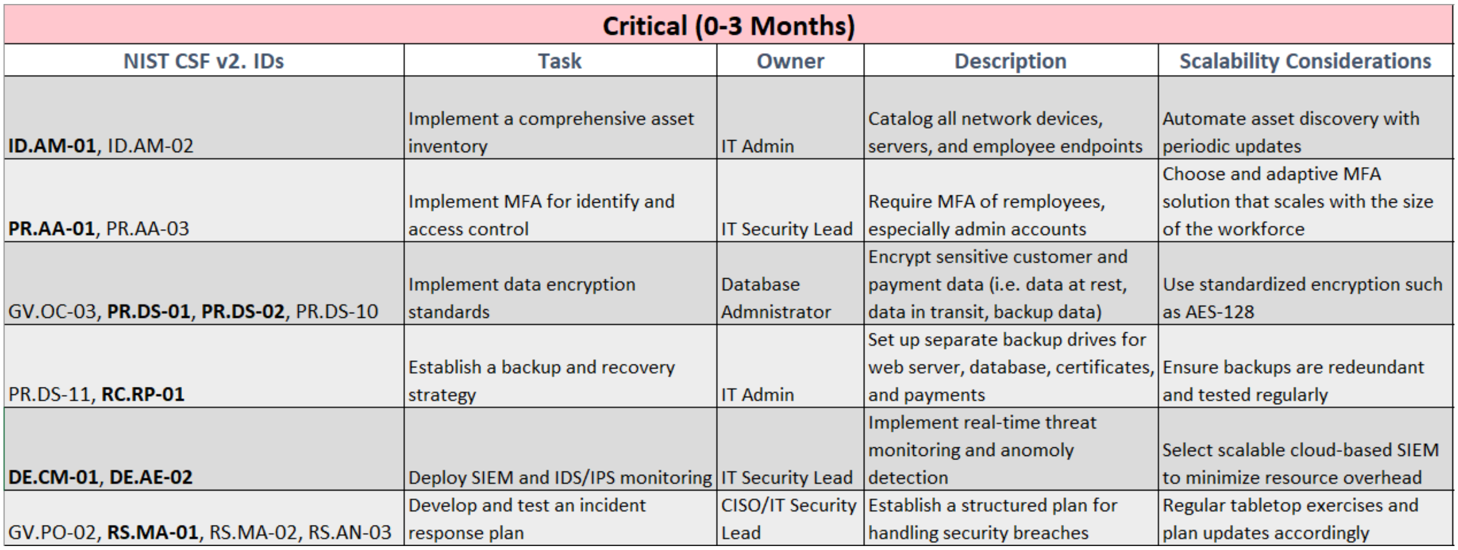


Function	Category	Subcategory
IDENTIFY (ID)	Asset Management	ID.AM-01: Asset Inventory
	Risk Assessment	ID.RA-01: Risk Assessment Process
		ID.RA-02: Cyber threat intelligence feeds and sources
	Improvement	ID-IM-01: Improvements made from evaluations
		ID-IM-04 - Incident repsonse plans established, communicated, maintained, improved
PROTECT (PR)	Identity Management, Authentication, Access Control	PR.AA-01: Identity and Access Management
	Awareness and Training	PR.AT-01: Security Awareness Training
	Data Security	PR.DS-01: Data encryption at rest
		PR.DS-02: Data encrption in transit
		PR.DS-04: Data backups are protected
	Platform Security	PR.PS-03: Software maintenance
	Technology Infrastructure Resliiance	PR.IR-01: Network protection from unauthroized access and usage
DETECT (DE)	Continous Monitoring	DE.CM-01: Security continuous monitoring
	Adverse Event Analysis	DE.AE-02: Anomoly detection and monitoring
RESPOND (RS)	Incident Management	RS.MA-01: Incident response plan execution
RECOVER (RC)	Incident Recovery Plan Execution	RC.RP-01: Recovery plan
	Incident Recovery Communication	RC.CO-03: Recovery steps communication

Figure 2.1 – NIST CSF v2. Recommended actions for the organization.

CRITICAL (0-3 MONTHS)

Objective: Address fundamental security vulnerabilities that pose immediate risks to business continuity and data security.

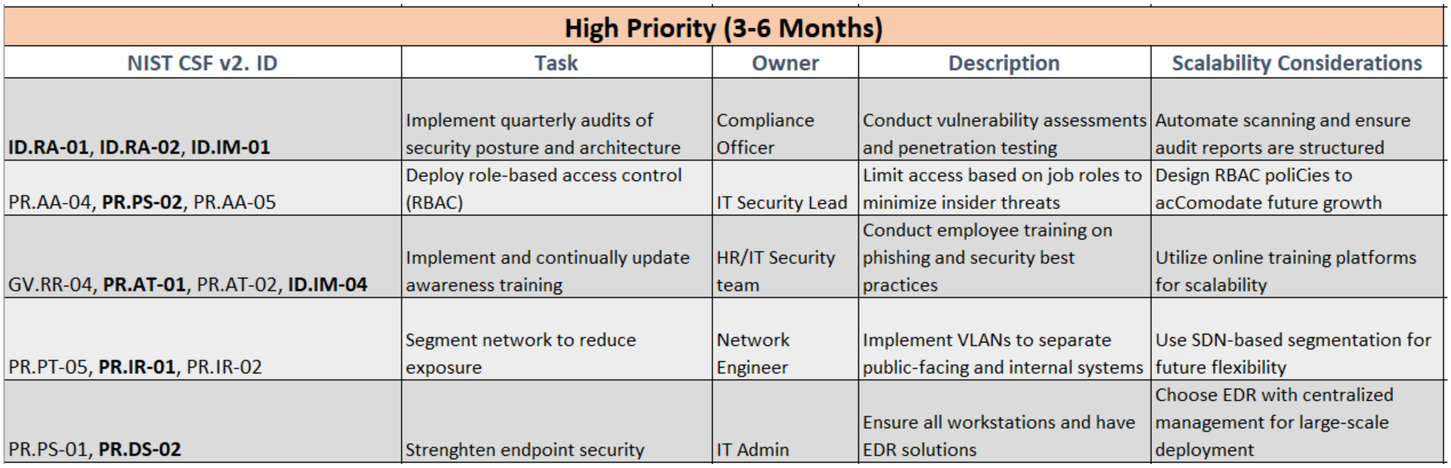


Critical (0-3 Months)				
NIST CSF v2. IDs	Task	Owner	Description	Scalability Considerations
ID.AM-01, ID.AM-02	Implement a comprehensive asset inventory	IT Admin	Catalog all network devices, servers, and employee endpoints	Automate asset discovery with periodic updates
PR.AA-01, PR.AA-03	Implement MFA for identify and access control	IT Security Lead	Require MFA of remployees, especially admin accounts	Choose and adaptive MFA solution that scales with the size of the workforce
GV.OC-03, **PR.DS-01**, **PR.DS-02**, PR.DS-10	Implement data encryption standards	Database Admnistrator	Encrypt sensitive customer and payment data (i.e. data at rest, data in transit, backup data)	Use standardized encryption such as AES-128
PR.DS-11, **RC.RP-01**	Establish a backup and recovery strategy	IT Admin	Set up separate backup drives for web server, database, certificates, and payments	Ensure backups are redeundant and tested regularly
DE.CM-01, **DE.AE-02**	Deploy SIEM and IDS/IPS monitoring	IT Security Lead	Implement real-time threat monitoring and anomoly detection	Select scalable cloud-based SIEM to minimize resource overhead
GV.PO-02, **RS.MA-01**, RS.MA-02, RS.AN-03	Develop and test an incident response plan	CISO/IT Security Lead	Establish a structured plan for handling security breaches	Regular tabletop exercises and plan updates accordingly

Figure 2.2 – Critical recommendations in need of immediate attention.

HIGH PRIORITY (3-6 MONTHS)

Objective: Strengthen risk management, detection, and response capabilities and effectiveness.

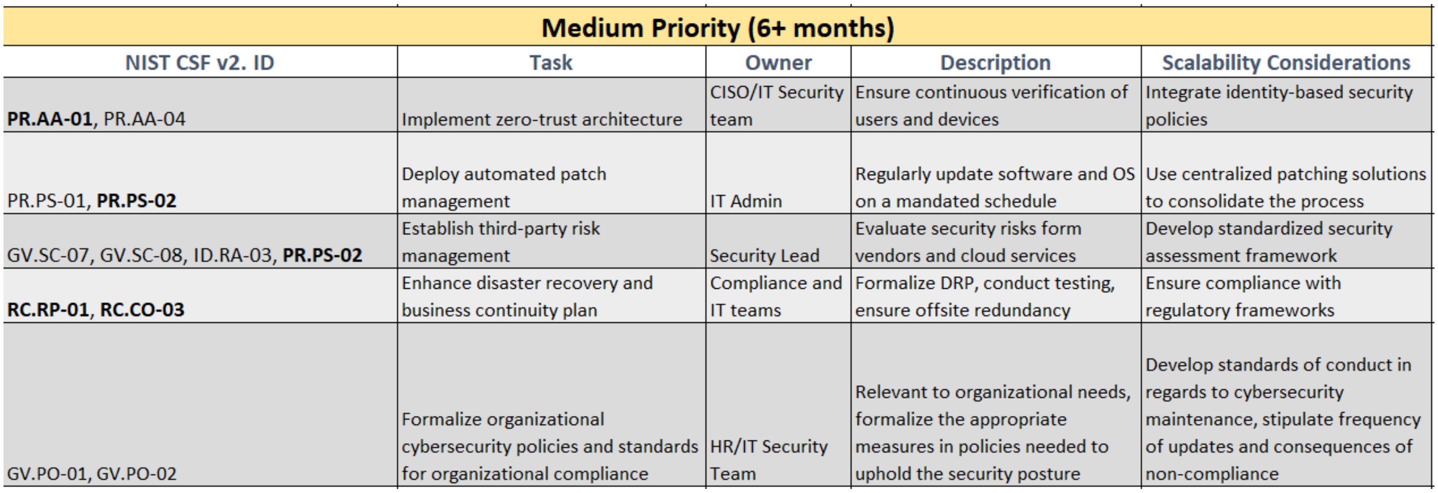


High Priority (3-6 Months)				
NIST CSF v2. ID	Task	Owner	Description	Scalability Considerations
ID.RA-01, **ID.RA-02**, **ID.IM-01**	Implement quarterly audits of security posture and architecture	Compliance Officer	Conduct vulnerability assessments and penetration testing	Automate scanning and ensure audit reports are structured
PR.AA-04, **PR.PS-02**, PR.AA-05	Deploy role-based access control (RBAC)	IT Security Lead	Limit access based on job roles to minimize insider threats	Design RBAC poliCies to acComodate future growth
GV.RR-04, **PR.AT-01**, PR.AT-02, **ID.IM-04**	Implement and continually update awareness training	HR/IT Security team	Conduct employee training on phishing and security best practices	Utilize online training platforms for scalability
PR.PT-05, **PR.IR-01**, PR.IR-02	Segment network to reduce exposure	Network Engineer	Implement VLANs to separate public-facing and internal systems	Use SDN-based segmentation for future flexibility
PR.PS-01, **PR.DS-02**	Strenghten endpoint security	IT Admin	Ensure all workstations and have EDR solutions	Choose EDR with centralized management for large-scale deployment

Figure 2.3 – High priority recommendations in need of attention soon after the critical gaps have been addressed.

MEDIUM PRIORITY (6+ MONTHS)

Objective: Enhance security governance, scalability, and operational resilience.

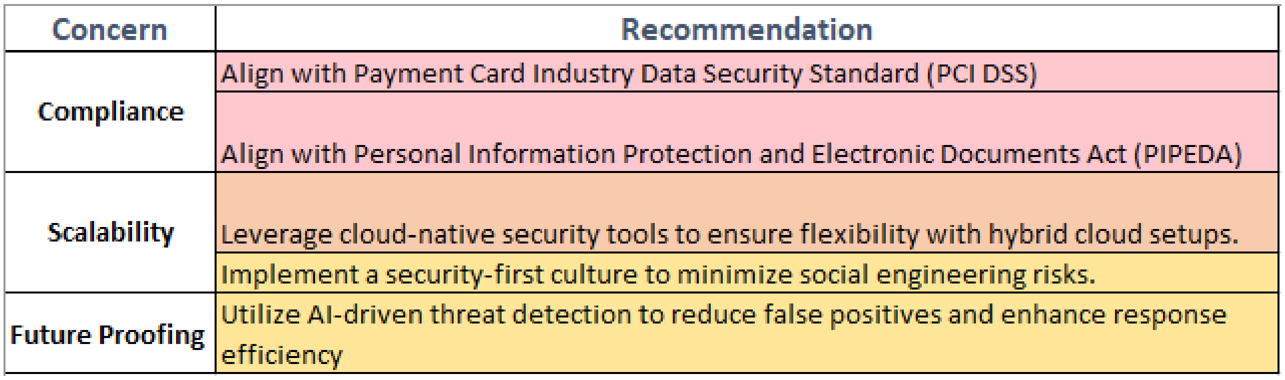


Medium Priority (6+ months)				
NIST CSF v2. ID	Task	Owner	Description	Scalability Considerations
PR.AA-01, PR.AA-04	Implement zero-trust architecture	CISO/IT Security team	Ensure continuous verification of users and devices	Integrate identity-based security policies
PR.PS-01, **PR.PS-02**	Deploy automated patch management	IT Admin	Regularly update software and OS on a mandated schedule	Use centralized patching solutions to consolidate the process
GV.SC-07, GV.SC-08, ID.RA-03, **PR.PS-02**	Establish third-party risk management	Security Lead	Evaluate security risks form vendors and cloud services	Develop standardized security assessment framework
RC.RP-01, **RC.CO-03**	Enhance disaster recovery and business continuity plan	Compliance and IT teams	Formalize DRP, conduct testing, ensure offsite redundancy	Ensure compliance with regulatory frameworks
GV.PO-01, GV.PO-02	Formalize organizational cybersecurity policies and standards for organizational compliance	HR/IT Security Team	Relevant to organizational needs, formalize the appropriate measures in policies needed to uphold the security posture	Develop standards of conduct in regards to cybersecurity maintenance, stipulate frequency of updates and consequences of non-compliance

Figure 2.4 – Medium priority recommendations in need of attention but can wait when more pressing areas of concern are addressed first.

ADDITIONAL CONSIDERATIONS

Below are additional considerations that are not outlined within the NIST CSF v2. Following a similar principle in determining tasks' priority levels, the colours below reflect how highly they are recommended given the current state of the organization, considering both budgetary and timely constraints. It is by no means extensive given the comprehensive analysis and recommendations given, the following table's contents are simple offered as a supplementary measure to further fortify the organization's security posture.



Concern	Recommendation
Compliance	Align with Payment Card Industry Data Security Standard (PCI DSS)
	Align with Personal Information Protection and Electronic Documents Act (PIPEDA)
Scalability	Leverage cloud-native security tools to ensure flexibility with hybrid cloud setups.
	Implement a security-first culture to minimize social engineering risks.
Future Proofing	Utilize AI-driven threat detection to reduce false positives and enhance response efficiency

Figure 2.6 – Additional considerations for implementation in conjunction with previous recommendations made within this report.

CONCLUSION

The current security posture of the organization reveals significant foundational gaps that must be addressed to establish a more resilient and practical network within today's evolving threat landscape. Key vulnerabilities identified include a reliance on a single physical server, inadequate network segmentation between public-facing and internal operations, and the absence of modern security standards such as continuous monitoring, incident response planning, contingency strategies, and patch management. These deficiencies created an environment susceptible to various security risks. To mitigate these threats, a structured roadmap has been developed, tailored specifically to the needs of a medium-sized organization. The roadmap prioritizes tasks based on urgency, with critical actions recommended for completion within 3 months, high-priority initiatives within 3-6 months, and medium-priority improvements scheduled beyond 6 months. While it is advisable to review the roadmap for potential customization or additional considerations, swift action is essential to address these substantial gaps in the organization's security architecture effectively.

REFERENCES

Hashemi-Pour, C. (2023, December). *What is the CIA triad (confidentiality, integrity and availability)?* . Retrieved from TechTarget: https://www.techtarget.com/whatis/definition/Confidentiality-integrity-and-availability-CIA

National Institute of Standards and Technology. (2012). *Guide for Conductin Risk Assessments.* National Institute of Standards and Technology.

National Institute of Standards and Technology. (2024). *NIST Cybersecurity Framework.* National Institute of Standards and Technology.