CyberTech Innovations NIST RMF

Initial Assessment

I will focus on CyberTech Innovations' Customer Data Management System (CDMS). This system utilizes a combination of cloud-based storage solutions and local data centers. It also performs data processing as well as analytics and has front-end interfaces developed in React.js. Potential risks surrounding this information system are unauthorized access resulting in a data breach, data inaccessibility, and service disruption. Potential threats that may increase these risks are phishing attacks targeting employees with access to the CDMS, ransomware attacks encrypting critical customer data, and DDoS attacks against public-facing applications. Potential vulnerabilities that may lead to these risks include but are not limited to poor employee awareness of phishing tactics, weak password practices, unpatched software vulnerabilities, lack of perimeter security controls, poor user access controls, and weaknesses in web security. The only controls noted in this assigned scenario are access controls.

RMF Implementation Plan

Introduction

CyberTech Innovations is a technology company specializing in innovative solutions in AI, IoT, and blockchain across various industries such as healthcare, finance, and manufacturing. The mission of CyberTech is to revolutionize how industries operate while ensuring the company has the highest cybersecurity standards. Implementing the NIST RMF is crucial for CyberTech Innovations because it ensures the security and resilience of their information systems. It provides a systematic approach to identify, assess, and mitigate risks, ultimately safeguarding their data, reputation, and business operations. The objectives of the RMF implementation plan are to manage risk and protect their information systems, and I will particularly focus on their CDMS.

Categorization of Information System

Table 1. FIPS 199 Impact Level Analysis

Impact Level	Confidentiality	Integrity	Availability
Low Impact	Unauthorized disclosure could cause limited harm.	Unauthorized modification could cause limited harm.	Disruption of access could cause limited harm.
Moderate Impact	Unauthorized disclosure could	Unauthorized modification could	Disruption of access could cause serious

	cause significant disruption to operations but is not catastrophic.	cause serious harm but not catastrophic.	harm but not catastrophic.
High Impact	Unauthorized disclosure could cause severe or catastrophic harm, e.g., customer financial data.	Unauthorized modification could result in financial inaccuracies, e.g., transaction records.	Disruption in access could prevent transactions, affecting customer trust and operational continuity.

Table 2. Impact Ratings

Information System	Confidentiality	Integrity	Availability
CDMS	Moderate Impact	Moderate Impact	High Impact

Rationale for Each Information System Impact Rating

1. CDMS
    a. **Confidentiality**: Moderate impact because unauthorized disclosure could cause significant disruption to operations. I did not categorize it as high impact because the data within the CDMS is PII and not sensitive data that could cause severe harm to the company's reputation and result in a loss of customer trust.
    b. **Integrity**: Moderate impact because unauthorized modifications to customer data may disrupt business operations as the information in the CDMS may not be as trustworthy. Therefore, the company would need to spend time validating its data if there isn't a proper backup in place.
    c. **Availability**: High impact because disruption in access could affect operational continuity which would prevent transactions, affecting customer trust.

Summary of Risks, Threats, and Vulnerabilities impacting CyberTech's CIA

1. **Summary of risk, threat, and vulnerabilities impacting confidentiality**
    a. Potential risk to confidentiality: Unauthorized access resulting in a data breach
    b. Potential threat to confidentiality: Phishing attacks targeting employees with access to the CDMS.
    c. Potential vulnerability to confidentiality: Poor employee awareness of phishing tactics, poor user access controls, and weak password practices.

2. **Summary of risk, threat, and vulnerabilities impacting integrity**
    a. Potential risk to integrity: Data inaccessibility.
    b. Potential threat to integrity: Ransomware attacks encrypting critical customer data.
    c. Potential vulnerability to integrity: Weak password practices, unpatched software vulnerabilities, and poor user access controls.

3. **Summary of risk, threat, and vulnerabilities impacting availability**
    a. Potential risk to availability: Service disruption.
    b. Potential threat to availability: DDoS attacks against public-facing applications.
    c. Potential vulnerability to availability: Weaknesses in web security such as lack of perimeter security controls, poorly configured servers, or outdated software.

Selection of Security Controls to Address Concerns to CyberTech's CIA

1. Control families to select security controls per NIST SP 800-53, Rev. 5: Access Control (AC), Awareness and Training (AT), Assessment, Authorization, and Monitoring (CA), Contingency Planning (CP), Identification and Authentication (IA), and Incident Response (IR), Maintenance (MA), Risk Assessment (RA), and System and Communications Protection (SC). Criteria for selecting security controls centered on addressing potential threats to CyberTech Innovations and ensuring CIA.

Table 3. Security Controls and Rationale

Security control	Rationale for selecting security control
AT-1	Security awareness training for all employees, covering phishing tactics such as how to identify suspicious emails, as well as how to identify and report potential ransomware attacks. Educate users on safe email practices and the importance of strong passwords to mitigate the risk of unauthorized access.
AT-2	Phishing simulation exercises to test employee awareness and response to phishing attempts to mitigate the risk of unauthorized access.
IA-2	Implement strong password requirements with complexity and regular password changes to mitigate the risk of unauthorized access.

IA-3	Implement the use of MFA to add an extra layer of security to logins to protect against phishing attacks in case an employee's login credentials have been successfully phished.
IR-1	Incident response plan with clear procedures for identifying, containing, and mitigating phishing incidents. Have procedures in place to isolate infected systems and contain the spread of ransomware.
IR-4	Have established incident response plans to quickly identify, contain, and remediate DDoS attacks to minimize system downtime.
AC-6	Implement least privilege access controls to limit user permissions based on their job function (use RBAC).
CA-7	Monitor user activity for suspicious patterns that could indicate phishing and ransomware attacks, like unusual login attempts or clicking on malicious links.
SC-5 (DoS Protection)	Focuses on implementing measures to mitigate the impact of DDoS attacks by utilizing techniques like boundary protection devices, increased bandwidth capacity, and service redundancy.
SC-7	Implements perimeter security controls like firewalls and IDS to filter incoming traffic.
SC-28	Implement cryptographic mechanisms to protect the confidentiality and integrity of data stored at rest, essentially requiring encryption and hashing for on-premise customer data storage.
CP-9	Establish and Implement procedures for backing up system information, including data restoration procedures.

RA-5	Monitor and scan for vulnerabilities in the system and hosted applications.
MA-3	This control ensures that the latest software updates and patches are installed. Pair with RA-5 to ensure the vulnerabilities detected are patched.
WAFs	Use to filter out malicious traffic targeting public-facing applications.

2. Since CyberTech Innovations operates in various industries it has to ensure it is compliant with major cybersecurity regulations such as HIPAA, GDPR, PCI-DSS, etc. The key compliance activities it has to meet are implementing risk assessments, access controls, data encryption methods, IRPs, employee training, and monitoring and logging. These controls address regulatory compliance requirements. Additionally, the controls address the identified vulnerabilities of the information system. It achieves this by having the stated control of conducting risk assessments and then ensuring the latest software updates and patches are installed.

Assessment Strategy

The security control assessments will involve vulnerability assessment, network assessment, and incident response simulations to phishing, ransomware, and DDoS attacks to ensure that the stated controls work effectively. The vulnerability and network assessments can take anywhere from a few days to several weeks to complete, depending on the size and complexity of the CDMS. The IT/cybersecurity team will be responsible for completing these assessments and simulations. Incident response simulations such as tabletop exercises are typically performed once a year and usually take between 2 to 4 hours to complete.

Milestones and Deliverables

NIST RMF Phase	Milestone	Deliverables
1. Categorize Information Systems	Define the system and determine its security impact level.	System Security Categorization FIPS 199 Impact Level Analysis Initial Risk Assessment
2. Select Security Controls	Choose applicable security controls based on the system's categorization.	Security Control Baseline Selection (per NIST SP 800-53)

		System Security Plan (SSP) - Initial Draft Risk Assessment Report (RAR)
3. Implement Security Controls	Deploy and configure security controls	Implementation Documentation System Configuration Settings Security Control Assessment Plan
4. Assess Security Controls	Evaluate security controls for effectiveness	Security Control Assessment Report Vulnerability Assessment Results Incident Response Simulations Results
5. Authorize Information System	Obtain authorization to operate (ATO) from the authorizing official	Final Risk Assessment Report (RAR) Authorization Decision Document (ATO or Denial)
6. Monitor Security Controls	Continuously track and manage security risks	Continuous Monitoring Plan Security Status Reports Incident Response Reports Periodic Risk Assessments

Risk Assessment Report

Executive Summary

This risk assessment process involves identifying the key assets of the CDMS and then identifying the potential risks, threats, and vulnerabilities to those key assets of the information system. After completing that, then a risk analysis will be performed which evaluates the likelihood of the risk and the impact of its consequences. Following this, the risks will be prioritized to determine which risks should be addressed first. Lastly, after prioritization of the risks, then appropriate mitigation strategies will be determined.

Methodology

The following risk assessment will utilize a combination of a qualitative and quantitative risk analysis methodology. Please reference Tables 4-7.

Risk Identification & Analysis

Table 4. Risk Matrix to Demonstrate How Risk Level is Calculated

		LIKELIHOOD		
RISK= LIKELIHOOD*IMPACT		Not likely (1)	Somewhat likely (2)	Very likely (3)
IMPACT	Not impactful (1)			
	Somewhat impactful (2)			
	Very impactful (3)			

Table 5. Risk Level Descriptions

Risk Level	Risk Description
Low (1-2)	A threat event could be expected to have a limited adverse effect on organizational operations, customers, or other organizations.
Moderate (3-4)	A threat event could be expected to have a serious adverse effect on organizational operations, customers, or other organizations.
High (5+)	A threat event could be expected to have a severe adverse effect on organizational operations, customers, or other organizations.

Table 6. Risk Likelihood Level Descriptions

Likelihood Level	Likelihood Description
Not likely (1)	Adversary is unlikely to initiate a threat event; Probable to occur only in rare circumstances, once in ten years or more
Somewhat likely (2)	Adversary is somewhat unlikely to initiate a threat event; Probable to occur within a year or two.
Very likely (3)	Adversary is highly likely to initiate a threat event; Probable to occur within weeks/months.

Table 7. Risk Impact Level Descriptions

Impact Level	Impact Description

Not impactful (1)	Minor financial loss (up to $25K); or range of effects is limited to some cyber resources but no critical resources.
Somewhat impactful (2)	Moderate financial loss ($25k - $500k); or range of effects is significant to some cyber resources and some critical resources.
Very impactful (3)	Major financial loss (over $500k); or range of effects is extensive to most cyber resources and most critical resources.

Table 8. Risks, Threats, and Vulnerabilities to CDMS & Associated Risk Level

	Risk	**Threats**	**Vulnerabilities**	**Risk Level**
Customer Database Management System (CDMS)	Data breach resulting from unauthorized access	Phishing attacks targeting employees with access to the CDMS	Poor employee awareness of phishing tactics, poor user access controls, and weak password practices	Likelihood: Very likely (3) Impact: Not impactful (1) Risk Level: 3 - Moderate
	Data inaccessibility	Ransomware attacks encrypting critical customer data	Weak password practices, unpatched software vulnerabilities, and poor user access controls	Likelihood: Very likely (3) Impact: Very impactful (3) Risk Level: 9 - High
	Service disruption	DDoS attacks against public-facing applications	Weaknesses in web security such as lack of perimeter security controls, poorly configured servers, or outdated software	Likelihood: Very likely (3) Impact: Somewhat impactful (2) Risk Level: 6 - High

Risk Prioritization

Prioritizing the risk of data inaccessibility should be CyberTech Innovation's main focus because a threat event, that is very likely to occur, could be expected to have severe adverse effects on organizational operations, customers, and/or its vendors. After addressing this risk, CyberTech should focus on addressing the risk of service disruption because although it is very likely, it would be somewhat impactful if it were to occur. Lastly, the last risk to address is the risk of a data breach. The criteria used for prioritizing these risks are based on each of their risk levels.

Conclusion

This comprehensive risk assessment has identified several key cybersecurity risks associated with CyberTech Innovations' CDMS. These risks include data breaches due to unauthorized access, data inaccessibility, and service disruptions. Additionally, the assessment uncovered vulnerabilities contributing to each risk, resulting in varying risk levels. Ranked from highest to lowest risk, data inaccessibility poses the greatest risk, followed by service disruption and data breaches. The approach to managing these risks will involve developing targeted risk mitigation strategies, which will be outlined in the next section.

Risk Mitigation Strategies

Introduction

After identifying and analyzing risks, the next step is risk mitigation. The goal of risk mitigation is to actively reduce the likelihood and/or potential impact of the identified risks occurring by implementing security controls and protective measures. These strategies are designed to minimize damage from cyber threats by proactively addressing vulnerabilities within an organization's systems and data. For CyberTech Innovations, we will proceed with this next phase of the RMF by addressing risks in order of priority, as outlined in the Risk Assessment Report. First, we will mitigate the highest-risk concern—data inaccessibility—followed by service disruption and, finally, data breaches.

Risk Mitigation Approaches

There are four primary methods for mitigating risks: risk avoidance, risk reduction, risk transference, and risk acceptance. Each strategy is defined as follows:

- **Risk avoidance**: Taking action to prevent a risk from happening.
- **Risk reduction**: Implementing controls to minimize the likelihood or impact of a risk.
- **Risk transference**: Shifting the responsibility of a risk to a third party.

- **Risk acceptance**: Accepting that a risk will happen and managing it accordingly.

For each identified risk, we will employ a risk reduction strategy by implementing security controls per NIST SP 800-53.

Detailed Mitigation Strategies

Table 9. Risks with Detailed Mitigation Strategies

Risk	Detailed Description of the Mitigation Strategy	Justification for the Chosen Strategy	Steps for Implementation	Assigned Responsibilities
Data inaccessibility resulting from ransomware attacks encrypting critical customer data	We will employ a risk reduction strategy to address this risk. The controls implemented will include regular and secure data backups, network segmentation, ransomware awareness training, RBAC, patch management, and IRPs.	Secure backups ensure data can be restored without paying a ransom. Network segmentation limits the impact by isolating infected systems. Ransomware awareness training reduces the likelihood of employees clicking on malicious links that trigger ransomware downloads. RBAC limits the damage in case of a successful attack by restricting access privileges. Patch management eliminates vulnerabilities that ransomware exploits to gain entry. Incident response plans ensure a coordinated approach to containing an attack and restoring operations.	Implement a strict data backup policy, ensuring backups are encrypted, stored offline, and tested regularly. Enforce least privilege access controls (RBAC) to limit employee access to customer data. Enable network segmentation to isolate critical systems and prevent lateral movement of ransomware. Conduct mandatory ransomware awareness training to educate employees on recognizing phishing emails and malicious attachments. Apply timely security patches and updates to close vulnerabilities that ransomware exploits. Establish an IRP	IT Security Team – Deploy and manage backup solutions, network segmentation, and patch management. Database Administrators – Ensure backups are performed securely and tested for reliability. HR & Compliance Teams – Conduct ransomware awareness training and enforce security policies. Incident Response Team – Develop response plans, monitor for ransomware activity, and coordinate containment efforts. Employees – Complete security training, report

			that outlines containment, eradication, and recovery procedures. Conduct ransomware attack simulations to test response readiness and improve reaction time.	suspicious activity, and follow cybersecurity best practices.
Service disruption resulting from DDoS attacks against public-facing applications	We will employ a risk reduction strategy to address this risk. The controls implemented will include WAFs, Rate limiting and traffic filtering, redundant network infrastructure and load balancing, and IRP for DDoS attacks.	WAFs block malicious requests before they reach the application. Rate limiting reduces the impact of bot-driven attacks by capping request rates. Load balancing ensures availability by redirecting traffic to healthy servers during an attack. An IRP enables rapid action to identify and counteract threats in real time.	Implement a WAF to filter out malicious traffic targeting public-facing applications. Configure rate limiting and traffic filtering to control excessive request rates and block suspicious IPs. Implement load balancing and redundant network infrastructure to distribute traffic efficiently and prevent server overload. Enable network traffic monitoring and anomaly Detection using SIEM tools to identify attack patterns. Develop and test an IRP for DDoS attacks to ensure quick reaction to ongoing threats. Regularly conduct DDoS attack	IT Security Team – Deploy and manage DDoS protection, WAFs, and network monitoring tools. Network Administrators – Implement rate limiting, load balancing, and redundant infrastructure. Incident Response Team – Monitor and respond to active DDoS attacks, coordinating mitigation efforts. Public Relations & Communications Team – Manage stakeholder communications during service disruptions.

			simulations to test defenses and response readiness.	
Data breach resulting from phishing attacks targeting employees with access to the CDMS	We will employ a risk reduction strategy to address this risk. The controls implemented will include MFA, RBAC, security awareness training, simulated phishing exercises, and incident response.	MFA ensures that stolen credentials alone are not enough to gain access. RBAC limits the damage in case of a successful attack by restricting access privileges. Training and phishing simulations prepare employees to recognize and report phishing attempts. Incident response ensures a swift reaction if a breach attempt is detected.	Enforce MFA for all employees accessing the CDMS. Implement RBAC to ensure only authorized personnel can access sensitive customer data. Conduct mandatory phishing awareness training for employees with access to the CDMS. Launch simulated phishing exercises every quarter to test employee vigilance and provide feedback. Monitor login activity and anomalies using SIEM tools. Develop and enforce a phishing IRP, ensuring employees know how to report phishing attempts and security teams can respond swiftly.	IT Security Team – Implement and manage email security, MFA, SIEM monitoring, and access controls. CDMS Administrators – Ensure RBAC is correctly applied and limit user privileges. HR & Compliance Teams – Conduct and enforce phishing awareness training. Incident Response Team – Develop response plans, investigate incidents, and mitigate breaches. Employees with CDMS Access – Complete phishing awareness training and report suspicious emails immediately.

Monitoring and Review Plan

To ensure that these mitigation strategies remain effective, a continuous monitoring and evaluation process should be established. The general process for monitoring the effectiveness of these implemented strategies involves tracking performance metrics, implementing continuous monitoring tools, conducting regular tests and validation, and making necessary updates to

defenses based on emerging threats and post-attack reviews. See the following tables for the corresponding schedule for regular reviews and updates:

Table 10. Mitigation Strategies for Data Inaccessibility

Review Activity	Frequency	Responsible Team(s)
Backup Integrity Testing & Restoration Drills	Monthly	IT Security, IT Operations
Access Controls & Privileged Access Management (PAM) Review	Quarterly	IT Security, IAM Team
Security Patch & Vulnerability Management Review	Monthly	IT Security, Patch Management Team
IRP & Ransomware Playbook Testing	Semi-Annually	IR Team, IT Security
Ransomware Awareness Training	Bi-Annually	HR
Review & Update Data Encryption Policies	Annually	GRC Team, Compliance Officers

Table 11. Mitigation Strategies for Service Disruption

Review Activity	Frequency	Responsible Team(s)
DDoS Mitigation Effectiveness Review	Quarterly	IT Security, Network Operations
Traffic Analysis & Anomaly Detection Review	Monthly	Security Analysts, SOC Team
Firewall & WAF Rule Audits	Bi-Annual	IT Security, Network Admins
Simulated DDoS Attack (PenTesting)	Annually	Red Team, External Security Consultants
IRP Testing	Semi-Annually	IR Team, IT Security
Vendor Security Review (DDoS Protection Providers)	Annually	IT Security Procurement

Policy & Procedure Updates	Annually or After Major Incidents	GRC Team, Compliance Officers

Table 12. Mitigation Strategies for Data Breach

Review Activity	Frequency	Responsible Team(s)
Phishing Protection Review	Monthly	IT Security
Phishing Awareness Training & Simulated Attacks	Quarterly	Security Awareness Team, HR
MFA & Access Controls Review	Quarterly	IAM Team, IT Security
User Access & RBAC Audit	Semi-Annually	IAM Team, Compliance Officers
IRP for Phishing Attacks Testing	Semi-Annually	IR Team, IT Security
Review of SIEM Logs	Ongoing	SOC Team, Security Analysts

References

Balbix. (2025, January 16). *What is cyber risk mitigation?* Retrieved January 31, 2025, from https://www.balbix.com/insights/what-is-cyber-risk-mitigation

CSF Tools. (n.d.). *NIST SP 800-53: IR-5 incident monitoring.* Retrieved January 31, 2025, from https://csf.tools/reference/nist-sp-800-53/r4/ir/ir-5/

Farouk, U. (2023, October 25). *GRC Lab Series: Creating a Plan of Action and Milestones (POAM).* Medium. Retrieved from https://medium.com/@umarfarouk037/grc-lab-series-creating-a-plan-of-action-and-milestones-poam-b804e7943ac

Hyperproof. (n.d.). *NIST 800-53: Understanding the controls.* Retrieved January 31, 2025, from https://hyperproof.io/nist-800-53/

KPMG. (2023, July 17). *Understanding ransomware attack risks.* Retrieved from https://kpmg.com/us/en/articles/2023/ransomware-attack-risks.html

Monday.com. (2024, July 28). *Risk mitigation: Definition, strategies, and examples.* Retrieved January 31, 2025, from https://monday.com/blog/project-management/risk-mitigation/

National Institute of Standards and Technology (NIST). (2020). *Security and privacy controls for information systems and organizations (NIST Special Publication 800-53, Revision 5).* U.S. Department of Commerce. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

Purplesec. (2024, March). *Learn about phishing attacks.* Retrieved January 31, 2025, from https://purplesec.us/learn/phishing-attacks/

StandardFusion. (2017, July 29). *FedRAMP security levels: Low, moderate, and high.* Retrieved January 31, 2025, from https://www.standardfusion.com/blog/fedramp-low-moderate-high