Risk Management Case Study

Zehra Nur Ozer

June 2024

Table of Contents

1 Executive Summary

DHA Enterprise Inc. (DHAEI) is a software development company located in Durham Region, Ontario. It has several branch offices, including an upcoming Brampton branch. The company operates a single active directory domain (DHA.com).

The main office supports 1,500 users, while the branch offices' read-only domain controller (RODC) can file servers for approximately 200 users. Additionally, the company has 20 remote programmers who work with company-issued laptops from home offices.

The company created this risk management plan following the NIST risk management framework.

After identifying the assets and threats, the impact and likelihood scores are calculated to understand the severity level (Risk Assessment Table). According to the results presented, some of the primary threats to DHAEI have been included as cyber attacks (unauthorized access or phishing attacks), data breaches, and system failure.

Calculating the impact and likelihood levels determines a risk level to prioritize the threats. Within the acceptance criteria, the potential response is prepared for a risk treatment report. To mitigate the potential threats, residual risk scores are created.

According to the result, DHAEI must follow the steps below to minimize the impact of any potential impact.

- Data breaches can be a threat to the system. As scored 'High,' the solution might be a two-factor authentication.
- Unauthorized access to VPN servers can be a 'High' risk. Updating VPN configurations might help to mitigate the damage.
- The main office file server (FSI) can experience data loss. Even though the risk level is 'Moderate,' it is useful to implement daily system backups.
- The remote work laptops are vulnerable to theft. Encrypting all company-issued laptops can reduce the risk of any critical data.

There are more potential threats and vulnerabilities created as a document, which has been demonstrated in this plan.

In conclusion, the risk management plan for DHAEI ensures that the company is well-prepared to address and mitigate risks to its information systems.

2 Purpose, Scope and Users

The purpose of this Risk Assessment Plan is to identify, assess and manage the risk to minimize the potential impact on DHA Enterprise Inc. (DHAEI)

The main purpose of this project is to help minimize the impact of an incident on business operations and the company's information security. Additionally, identifying any risks and threats to information systems and developing strategies for mitigation to identified risks.

The scope of this project covers all technical, security, or user-related aspects within DHAEI. This includes the main office and the branches, including the new opening of the Brampton branch. As mentioned in the company's existing environment, the scope addresses infrastructure, servers, remote work, and data security.

The users are DHAEI's management team, IT department, including the branch office technical department as well as the remote workers and staff.

3 Risk Assessment and Risk Treatment Methodology

3.1 Risk Assessment

The risk assessment is the process of understanding, identifying, analyzing, and evaluating the Cyber Security risks. (Placeholder1)

3.1.1 The Process

The process to create the risk assessment is discussed in the following steps. The process is coordinated to identify threats, assets, and vulnerabilities performed by asset owners.

The identification task includes both assets and threats. First, all assets, such as servers, network infrastructure, devices, and data, are cataloged. Threats include cyber attacks, data breaches, system failures, and physical theft.

Network, systems and processes can be titled as the company's vulnerabilities.

3.1.2 Assets, vulnerability and threats

After analyzing DHAEI, the assets, vulnerabilities, and threats are determined.

Assets: Servers (DC1, DC2, FSI, WSUSI, DHADNS), laptops, desktops, and network infrastructure.

Vulnerabilities: Unpatched systems, weak control systems, weak physical security.

Threats: Cyber attacks, data breaches, system failures

3.1.3 Determining the risk owners

For each risk, a risk owner must be assigned. In DHAEI the company hierarchy can be divided into three segments to determine the risk owners. (nistgov)

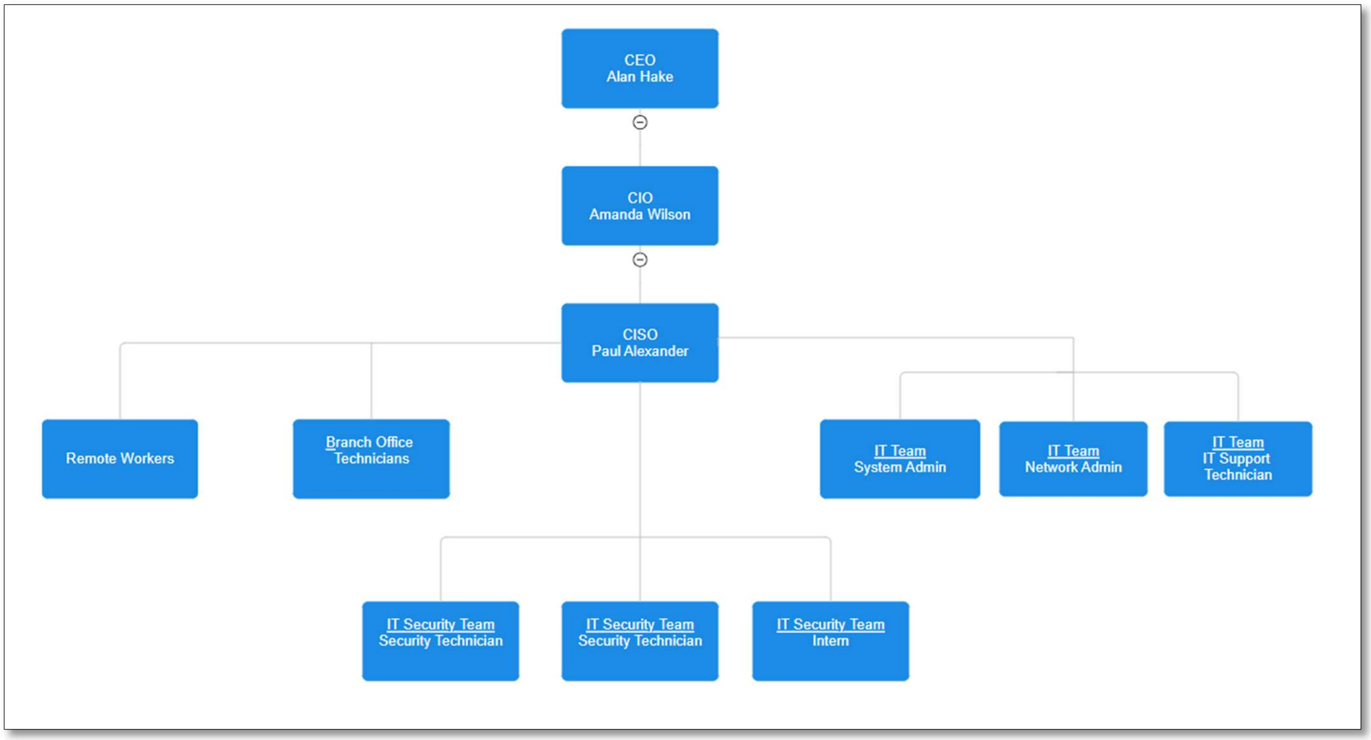
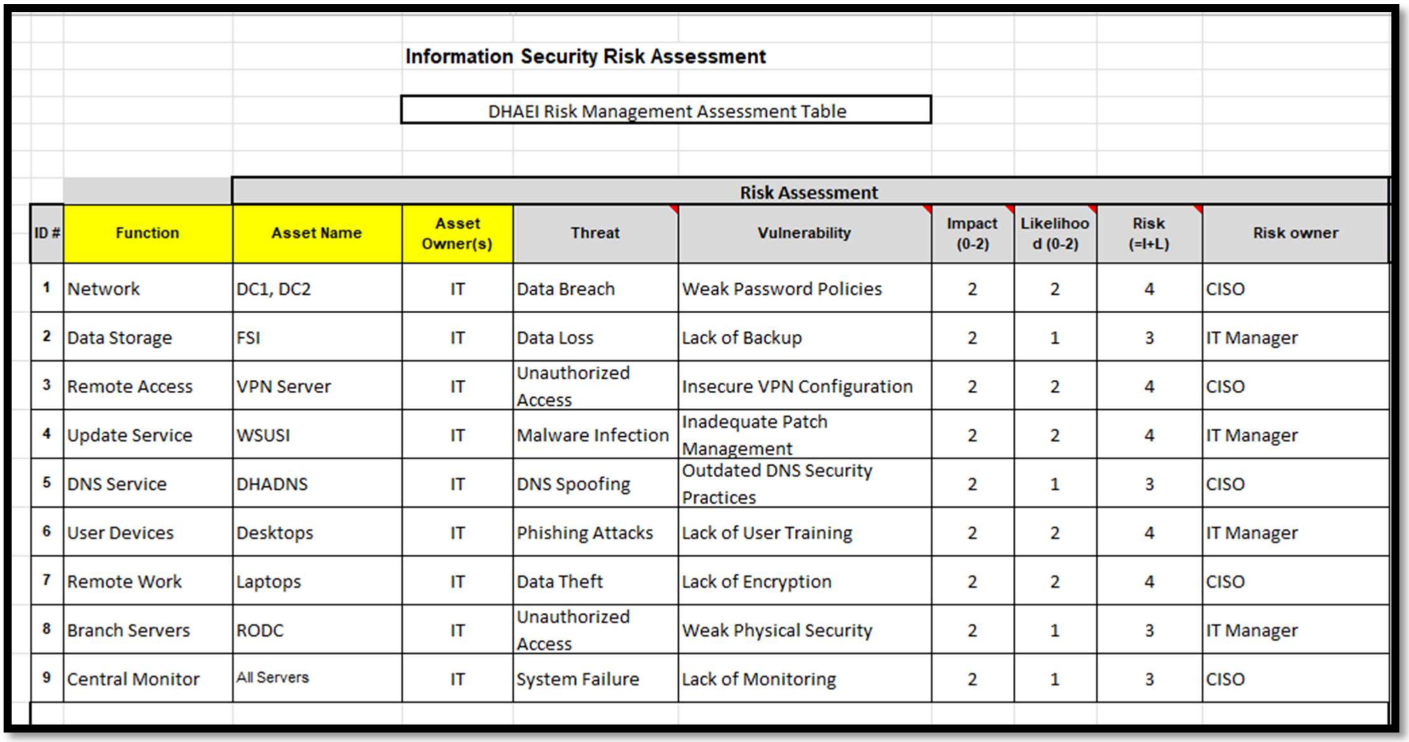


Figure 1. DHAEI IT Risk Management Hierarchy of Roles (smartdraw)

As identified in Figure 1 above, Branch officers are responsible for local maintenance. The IT Team is responsible for identifying and reporting vulnerabilities. CISO Paul Alexander oversees risk management and coordinates mitigation strategies. CIO Amanda Wilson adds the business objectives and reports to CEO Alan Hake.

3.1.4 Impact and Likelihood

After identifying the key assets and potential risks and considering the CIA Triad, the following risk assessment table (Table 1) was created.



Information Security Risk Assessment

DHAEI Risk Management Assessment Table

		Risk Assessment							
ID #	Function	Asset Name	Asset Owner(s)	Threat	Vulnerability	Impact (0-2)	Likelihood (0-2)	Risk (=I+L)	Risk owner
1	Network	DC1, DC2	IT	Data Breach	Weak Password Policies	2	2	4	CISO
2	Data Storage	FSI	IT	Data Loss	Lack of Backup	2	1	3	IT Manager
3	Remote Access	VPN Server	IT	Unauthorized Access	Insecure VPN Configuration	2	2	4	CISO
4	Update Service	WSUSI	IT	Malware Infection	Inadequate Patch Management	2	2	4	IT Manager
5	DNS Service	DHADNS	IT	DNS Spoofing	Outdated DNS Security Practices	2	1	3	CISO
6	User Devices	Desktops	IT	Phishing Attacks	Lack of User Training	2	2	4	IT Manager
7	Remote Work	Laptops	IT	Data Theft	Lack of Encryption	2	2	4	CISO
8	Branch Servers	RODC	IT	Unauthorized Access	Weak Physical Security	2	1	3	IT Manager
9	Central Monitor	All Servers	IT	System Failure	Lack of Monitoring	2	1	3	CISO

Table 1. Risk Assessment Table

3.1.5 Risk Acceptance Criteria

The impact and likelihood scores in the risk assessment table help to understand the acceptable benchmark for the risks.

Impact and Likelihood levels to the organizational unit if the threat materializes is scored as:

- (2) - High Impact
- (1) - Moderate Impact
- (0) - Low Impact

Considering the findings in the Risk Assessment Table, values for Risks are considered as:

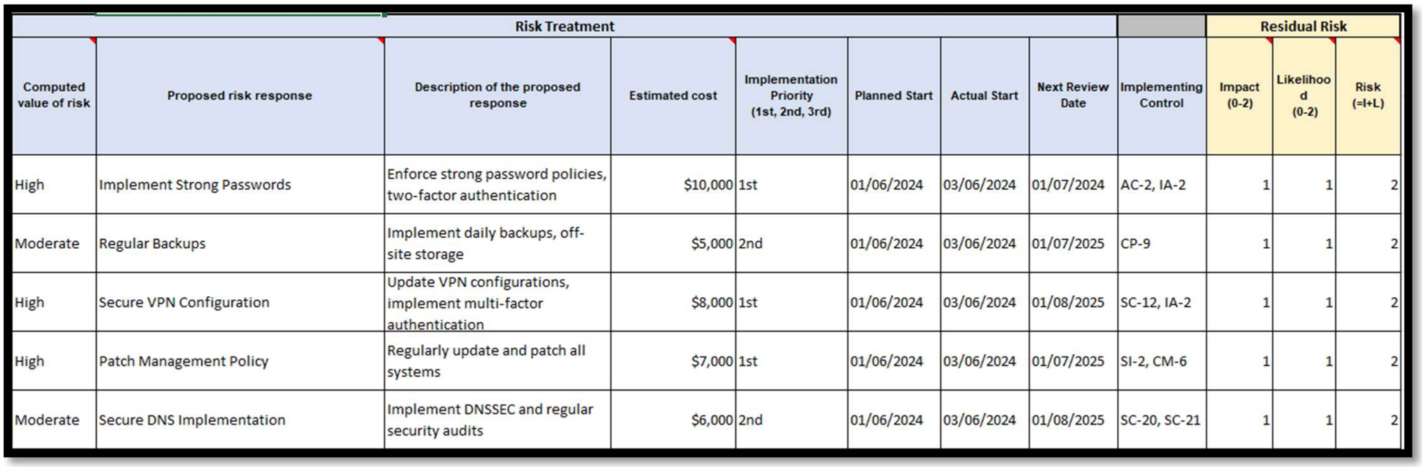
- (0) – Very Low Impact
- (1) – Low Impact
- (2) – Medium Impact
- (3) – High Impact
- (4) – Very High Impact

Columns scored as ‘3’ and ‘4’ in the Risk column should not be accepted and carefully reviewed and monitored.

3.2 Risk Treatment

After determining the Risk Score, the next step is to decide how to mitigate the risk. Implementing the proposed response can reduce the risk impact, and the residual risk score can be calculated again afterward.

Each potential threat is then addressed accordingly, using NIST 800-63B (Digital Identity Guidelines) as a reference.



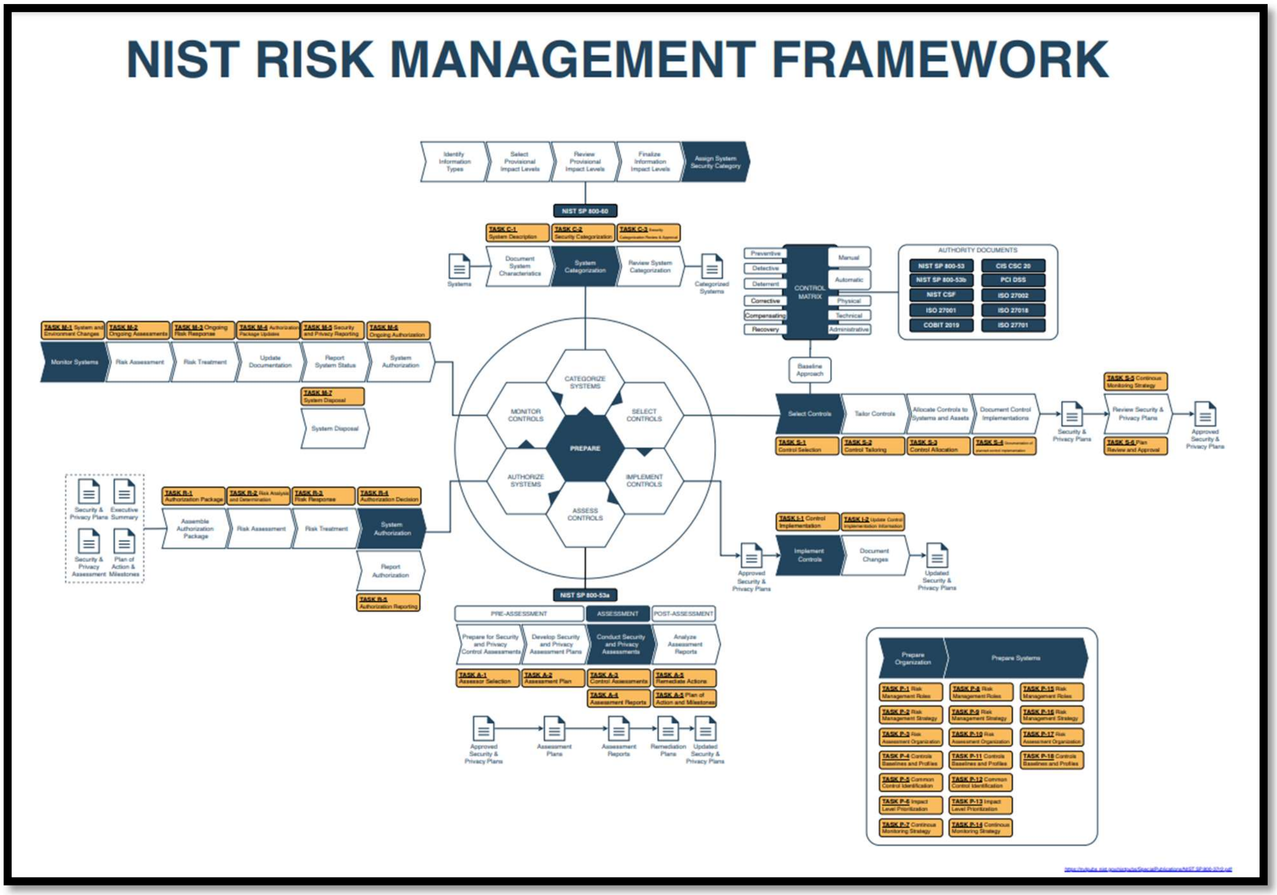
Risk Treatment									Residual Risk		
Computed value of risk	Proposed risk response	Description of the proposed response	Estimated cost	Implementation Priority (1st, 2nd, 3rd)	Planned Start	Actual Start	Next Review Date	Implementing Control	Impact (0-2)	Likelihood (0-2)	Risk (=I+L)
High	Implement Strong Passwords	Enforce strong password policies, two-factor authentication	$10,000	1st	01/06/2024	03/06/2024	01/07/2024	AC-2, IA-2	1	1	2
Moderate	Regular Backups	Implement daily backups, off-site storage	$5,000	2nd	01/06/2024	03/06/2024	01/07/2025	CP-9	1	1	2
High	Secure VPN Configuration	Update VPN configurations, implement multi-factor authentication	$8,000	1st	01/06/2024	03/06/2024	01/08/2025	SC-12, IA-2	1	1	2
High	Patch Management Policy	Regularly update and patch all systems	$7,000	1st	01/06/2024	03/06/2024	01/07/2025	SI-2, CM-6	1	1	2
Moderate	Secure DNS Implementation	Implement DNSSEC and regular security audits	$6,000	2nd	01/06/2024	03/06/2024	01/08/2025	SC-20, SC-21	1	1	2

Table 2. Risk Treatment Table

- The threat of data breach creates vulnerability due to weak password policies. NIST 800-63B recommends strong authentication methods, including multi-factor authentication. Implementing control code (AC-2 Account Management and IA-2 Identification and Authentication)
- Lack of backups threatens the system with data loss. NIST Special Publication 800-34 (Contingency Planning Guide for Federal Information Systems) emphasizes the importance of regular backups, which help protect the system from data loss.
- Remote access brings unauthorized access risk into the system. Securing VPN configurations and implementing multi-factor authentication can prevent this issue. MITRE ATT&CK framework identifies VPN-related vulnerabilities and suggests mitigation strategies.
- Regular patching reduces the risk of vulnerabilities and protects the system from malware infection. NIST Special Publication 800-40 (Guide to Enterprise Patch Management Technologies) outlines best practices for patch management.
- NIST Special Publication 800-81 (Secure Domain Name System (DNS) Deployment Guide) provides guidelines for secure DNS implementation to reduce the risk of DNS-based attacks.

4 Appendix:

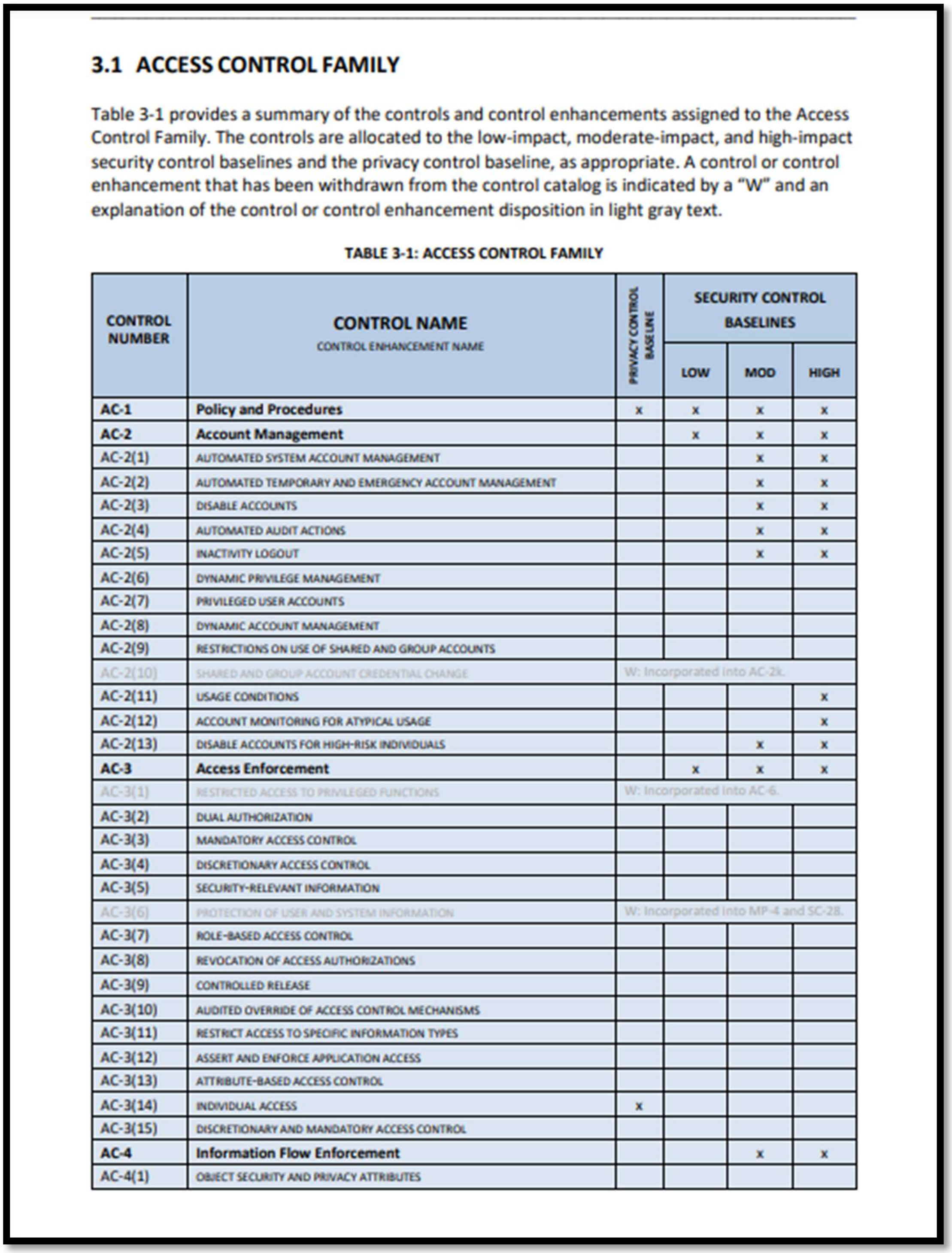
1. NIST Risk Management Framework


NIST RISK MANAGEMENT FRAMEWORK
Identify Information Types
Select Provisional Impact Levels
Review Provisional Impact Levels
Finalize Information Impact Levels
Assign System Security Category
NIST SP 800-60
TASK C-1 System Description
TASK C-2 Security Categorization
TASK C-3 Security Categorization Review & Approval
Systems
Document System Characteristics
System Categorization
Review System Categorization
Categorized Systems
Preventive
Detective
Deterrent
Corrective
Compensating
Recovery
CONTROL MATRIX
Manual
Automatic
Physical
Technical
Administrative
AUTHORITY DOCUMENTS
NIST SP 800-53
CIS CSC 20
NIST SP 800-53b
PCI DSS
NIST CSF
ISO 27002
ISO 27001
ISO 27018
COBIT 2019
ISO 27701
Baseline Approach
TASK M-1 System and Environment Changes
TASK M-2 Ongoing Assessments
TASK M-3 Ongoing Risk Response
TASK M-4 Authorization Package Updates
TASK M-5 Security and Privacy Reporting
TASK M-6 Ongoing Authorization
Monitor Systems
Risk Assessment
Risk Treatment
Update Documentation
Report System Status
System Authorization
TASK M-7 System Disposal
System Disposal
CATEGORIZE SYSTEMS
MONITOR CONTROLS
SELECT CONTROLS
PREPARE
AUTHORIZE SYSTEMS
IMPLEMENT CONTROLS
ASSESS CONTROLS
TASK S-5 Continous Monitoring Strategy
Select Controls
Tailor Controls
Allocate Controls to Systems and Assets
Document Control Implementations
Security & Privacy Plans
Review Security & Privacy Plans
Approved Security & Privacy Plans
TASK S-1 Control Selection
TASK S-2 Control Tailoring
TASK S-3 Control Allocation
TASK S-4 Documentation of planned control implementation
TASK S-6 Plan Review and Approval
Security & Privacy Plans
Executive Summary
Security & Privacy Assessment
Plan of Action & Milestones
TASK R-1 Authorization Package
TASK R-2 Risk Analysis and Determination
TASK R-3 Risk Response
TASK R-4 Authorization Decision
Assemble Authorization Package
Risk Assessment
Risk Treatment
System Authorization
Report Authorization
TASK R-5 Authorization Reporting
TASK I-1 Control Implementation
TASK I-2 Update Control Implementation Information
Approved Security & Privacy Plans
Implement Controls
Document Changes
Updated Security & Privacy Plans
NIST SP 800-53a
PRE-ASSESSMENT
ASSESSMENT
POST-ASSESSMENT
Prepare for Security and Privacy Control Assessments
Develop Security and Privacy Assessment Plans
Conduct Security and Privacy Assessments
Analyze Assessment Reports
TASK A-1 Assessor Selection
TASK A-2 Assessment Plan
TASK A-3 Control Assessments
TASK A-5 Remediate Actions
TASK A-4 Assessment Reports
TASK A-5 Plan of Action and Milestones
Approved Security & Privacy Plans
Assessment Plans
Assessment Reports
Remediation Plans
Updated Security & Privacy Plans
Prepare Organization
Prepare Systems
TASK P-1 Risk Management Roles
TASK P-8 Risk Management Roles
TASK P-15 Risk Management Roles
TASK P-2 Risk Management Strategy
TASK P-9 Risk Management Strategy
TASK P-16 Risk Management Strategy
TASK P-3 Risk Assessment Organization
TASK P-10 Risk Assessment Organization
TASK P-17 Risk Assessment Organization
TASK P-4 Controls Baselines and Profiles
TASK P-11 Controls Baselines and Profiles
TASK P-18 Controls Baselines and Profiles
TASK P-5 Common Control Identification
TASK P-12 Common Control Identification
TASK P-6 Impact Level Prioritization
TASK P-13 Impact Level Prioritization
TASK P-7 Continous Monitoring Strategy
TASK P-14 Continous Monitoring Strategy
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf

(By Aron Lange)

2. NIST.SP.800-53b

Control Baseline sample page.



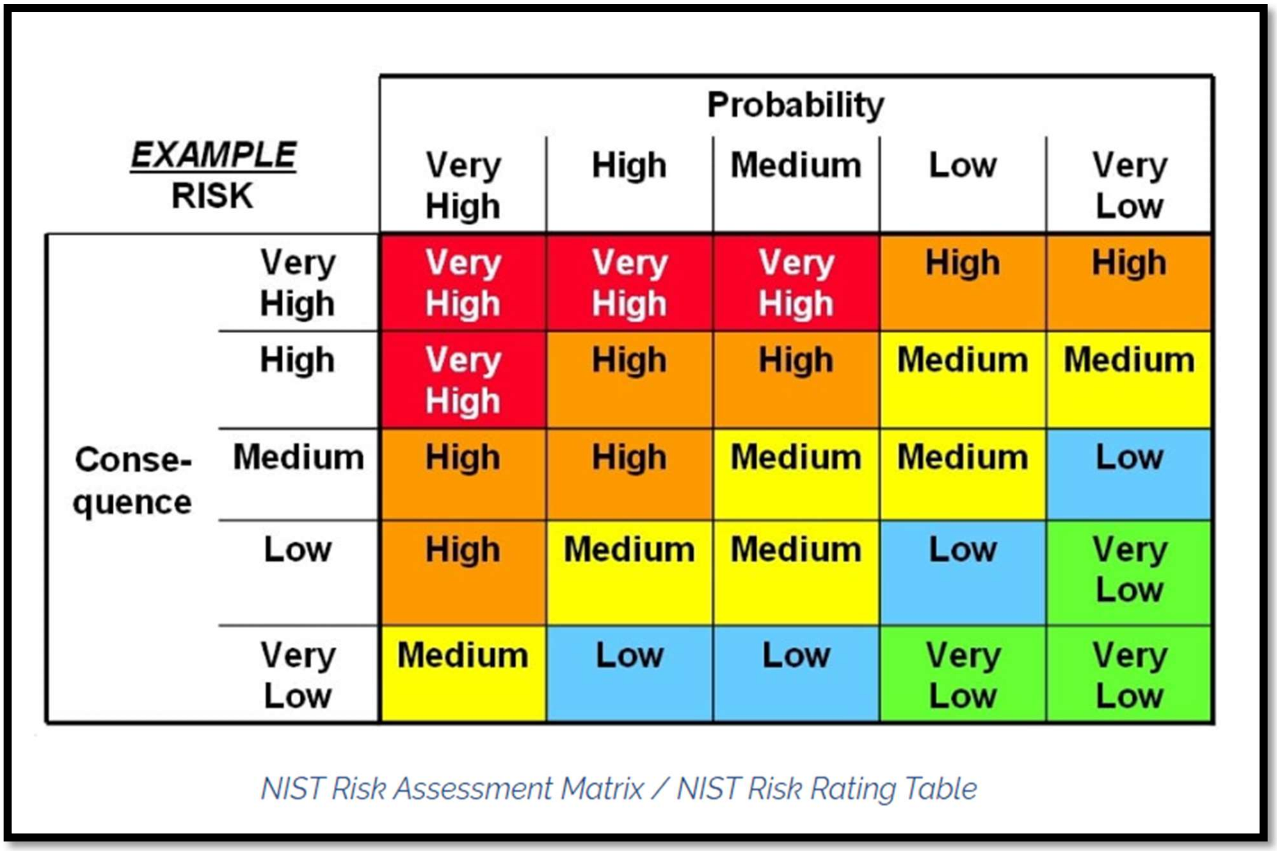
3.1 ACCESS CONTROL FAMILY

Table 3-1 provides a summary of the controls and control enhancements assigned to the Access Control Family. The controls are allocated to the low-impact, moderate-impact, and high-impact security control baselines and the privacy control baseline, as appropriate. A control or control enhancement that has been withdrawn from the control catalog is indicated by a "W" and an explanation of the control or control enhancement disposition in light gray text.

TABLE 3-1: ACCESS CONTROL FAMILY

CONTROL NUMBER	CONTROL NAME CONTROL ENHANCEMENT NAME	PRIVACY CONTROL BASELINE	SECURITY CONTROL BASELINES		
			LOW	MOD	HIGH
AC-1	**Policy and Procedures**	x	x	x	x
AC-2	**Account Management**		x	x	x
AC-2(1)	AUTOMATED SYSTEM ACCOUNT MANAGEMENT			x	x
AC-2(2)	AUTOMATED TEMPORARY AND EMERGENCY ACCOUNT MANAGEMENT			x	x
AC-2(3)	DISABLE ACCOUNTS			x	x
AC-2(4)	AUTOMATED AUDIT ACTIONS			x	x
AC-2(5)	INACTIVITY LOGOUT			x	x
AC-2(6)	DYNAMIC PRIVILEGE MANAGEMENT				
AC-2(7)	PRIVILEGED USER ACCOUNTS				
AC-2(8)	DYNAMIC ACCOUNT MANAGEMENT				
AC-2(9)	RESTRICTIONS ON USE OF SHARED AND GROUP ACCOUNTS				
AC-2(10)	SHARED AND GROUP ACCOUNT CREDENTIAL CHANGE	W: Incorporated into AC-2k.			
AC-2(11)	USAGE CONDITIONS				x
AC-2(12)	ACCOUNT MONITORING FOR ATYPICAL USAGE				x
AC-2(13)	DISABLE ACCOUNTS FOR HIGH-RISK INDIVIDUALS			x	x
AC-3	**Access Enforcement**		x	x	x
AC-3(1)	RESTRICTED ACCESS TO PRIVILEGED FUNCTIONS	W: Incorporated into AC-6.			
AC-3(2)	DUAL AUTHORIZATION				
AC-3(3)	MANDATORY ACCESS CONTROL				
AC-3(4)	DISCRETIONARY ACCESS CONTROL				
AC-3(5)	SECURITY-RELEVANT INFORMATION				
AC-3(6)	PROTECTION OF USER AND SYSTEM INFORMATION	W: Incorporated into MP-4 and SC-28.			
AC-3(7)	ROLE-BASED ACCESS CONTROL				
AC-3(8)	REVOCATION OF ACCESS AUTHORIZATIONS				
AC-3(9)	CONTROLLED RELEASE				
AC-3(10)	AUDITED OVERRIDE OF ACCESS CONTROL MECHANISMS				
AC-3(11)	RESTRICT ACCESS TO SPECIFIC INFORMATION TYPES				
AC-3(12)	ASSERT AND ENFORCE APPLICATION ACCESS				
AC-3(13)	ATTRIBUTE-BASED ACCESS CONTROL				
AC-3(14)	INDIVIDUAL ACCESS	x			
AC-3(15)	DISCRETIONARY AND MANDATORY ACCESS CONTROL				
AC-4	**Information Flow Enforcement**			x	x
AC-4(1)	OBJECT SECURITY AND PRIVACY ATTRIBUTES				

3. NIST Risk Assessment Matrix



EXAMPLE **RISK**		**Probability**				
		Very High	**High**	**Medium**	**Low**	**Very Low**
Consequence	**Very High**	Very High	Very High	Very High	High	High
	High	Very High	High	High	Medium	Medium
	Medium	High	High	Medium	Medium	Low
	Low	High	Medium	Medium	Low	Very Low
	Very Low	Medium	Low	Low	Very Low	Very Low

NIST Risk Assessment Matrix / NIST Risk Rating Table

(fortifydata)

5 References

https://fortifydata.com/blog/what-is-the-nist-rating-scale/

Gerald Auger, P. -S. (2023). *youtube.com*. Retrieved from https://www.youtube.com/watch?v=Z2okRecJC7E

https://chatgpt.com/. (2024). Retrieved from https://chatgpt.com/

LighthouseLab. (2024). *compass.lighthouselabs.ca*. Retrieved from https://web.compass.lighthouselabs.ca/p/14/ff8dfc8b-80e4-4c37-b18b-6aaac8883294

lighthouselabs. (2024). *Risk Management Plan*. Retrieved from https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C5/Cyber+BC+C5.2/Sample+Risk+Management+Plan.pdf

lighthouselabs. (2024). *Sample IT Asset Table*. Retrieved from https://learningimages.lighthouselabs.ca/Cyber+BC/Cyber+BC+C5/Cyber+BC+C5.1/Asset+Table+Example.pdf

nist.gov. (2020, Sep). *Security and Privacy Controlsfor*. Retrieved from https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r5.pdf

smartdraw. (2024). Retrieved from https://app.smartdraw.com/editor.aspx?templateId=dbc0cf47-3859-4a06-9f2a-972dc397fe12&flags=128#depoId=57913212&credID=-64805140

STANDARDS, N. I. (2008). *INFORMATIONSECURITY*. Retrieved from https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-60v2r1.pdf