



**Northeastern
University**

CY5200: Security Risk Management and Assessment



Instructor: [REDACTED]

Student: Davindernain Singh Sehgal

NUID: [REDACTED]

Table of Contents

Part	Title	Page No.
Part A	Security Risk Management Assessment	4
	Executive Summary	5
	List of Assets (\$)	8
	List of Threats	9
	List of Vulnerabilities	9
	Asset Vulnerability pairs	10
	Threat/Vulnerability Pairs Probabilities considering asset subset	10
	HGA's Current Security Controls and Policies List	10
	HGA's New CISO Recommended Security Controls and policies list	12
	Security Risk Prevention Strategy	13
	Security Risk Response (resilience) Strategy	20
	Mixed Security Risk Prevention Strategy and Security Risk Response (Resilience Strategy)	28
	Conclusion: Cost Benefit Analysis	31
Part B	Security Risk Management Implementation Plan	33
	Access Control Security Risk Management Implementation Controls and Policies	34
	Network Infrastructure Security Risk Management Implementation Controls and Policies	35
	Network Infrastructure Management Security Risk Management Implementation Controls and Policies	36
	Database Security Risk Management Implementation Controls and Policies	38
	Applications Development Security Risk Management Implementation Controls and Policies	40
	Wireless Security Risk Management Implementation Controls and Policies	41
	List of Cybersecurity implementation controls that exist at autumn-CSTL	43
	Comparison of the Implementation controls discussed in class with Autumn-CSTL Cybersecurity Implementation Controls	49
	List of Critical assets that exist in your company	56
	List of potential vulnerabilities for critical assets where cybersecurity implementation controls are missing	56
	List of potential threats to your company that could exploit vulnerabilities of critical assets	56
	List of potential risks for critical assets where cybersecurity implementation controls are missing	57
	List of recommended Hardening prevention controls and policies	57
	List of Recommended Hardening response controls and policies for critical assets	58
	Applicable Government Regulations and Industry Standards	59
	Rank asset risks and vulnerability risks of Autumn-CSTL	61
	List of cybersecurity Specialty areas that exist in Autumn-CSTL	63
	List of cybersecurity work roles that exist in your company	63
	List of Cybersecurity tasks that exist in your company	64

	Comparison of the NCWF recommended cybersecurity Specialty Areas with Autumn-CSTL's Existing Cybersecurity Specialty Areas	72
	Comparison of the NCWF recommended cybersecurity Work roles with Autumn-CSTL's Existing Cybersecurity work roles	73
	Comparison of the NCWF recommended cybersecurity tasks with Autumn-CSTL's Existing Cybersecurity Tasks	73
	List of potential threats to Autumn-CSTL that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, cybersecurity work roles, and cybersecurity tasks	119
	List of potential risks for critical assets where cybersecurity Specialty areas, Cybersecurity Work Roles, and Cybersecurity tasks are missing	119
	List of recommended policies for each recommended cybersecurity specialty area, Cybersecurity work role, or cybersecurity task that should be created to mitigate the identified risks.	120
Part C	Security Risk Management Recommendations	121
	List of recommended prevention and response controls, methods and policies and their implementation costs and benefits	122
	Provide the total cost and benefit in \$ for the recommended controls, methods, and policies	123
	Comparison of proposed security controls, methods and policies budget for HGA with the proposed security controls, methods and policies budget for Autumn-CSTL	123
	Attack Tree for HGA	124
	Attack Tree for Autumn-CSTL	125
	Vulnerabilities and exploitation probabilities	125
	Cybersecurity workforce recommendation	126
Part D	Appendix	127
	Appendix 3: Detailed Network Topology for HGA	128
	Appendix 4: Detailed Network Topology (defense0in-depth) for autumn-CSTL	128
	References	130

PART A : Security Risk Management Assessment

Executive Summary

Information System Name: Hypothetical Government Agency

Information System Categorization:

Assets	Information Security Elements		
	Confidentiality (C)	Integrity (I)	Availability (A)
Financial Documents	High	High	High
Timesheets	High	High	High
System Components	High	High	High
Business Documents	High	High	High
Procurement Documents	High	High	High
Regulatory & Compliance Documents	High	High	High
Personally Identifiable Information (PII)	High	High	High

Organization Name: Hypothetical Government Agency

Organization Address: 338 Huntington Ave, Boston, 02115

James Cameron

Title: Chief Executive Officer

Email: Cameron.j@gmail.com

Phone: +1 210-324-5445

Pavitra Prabhakar

Title: Chief Information Officer

Email: Prabhakar.p@gmail.com

Phone: +1 617-344-2312

Bucky Barnes

Title: Chief Financial Officer

Email: barnes.b@gmail.com

Phone: +1 210-311-3425

Ramesh Babu

Title: Chief Information Security Officer

Email: babu.r@gmail.com

Phone: +1 210-322-1245

Information System Operational Status: operational

Information System Type: Major Application

System Description: Funds Transfer from the US government to individual customer

System Environment: Refer to appendix

Interconnection of System Information:

System Name: Government Agency

Type of Organization: Public sector telecommunication industry

Type of Agreement: government contract

Date: March 31, 1998

FIPS 199 Category: High (H)

C&A Category: Accredited and certified

Authorizing Official: Regina Phalange

Following is the list of all the applicable laws/frameworks/standards/policies and regulations:

- Federal Trade Commission's (FTC) Safeguards Rule
- US Privacy Act of 1974
- California Consumer Privacy Act
- Sarbanes-Oxley Act
- Gramm-Leach-Bliley Act (GLBA)
- ISO 27001 – Information Security Management Systems
- ISO 22301 – Security and resilience – Business Continuity Management Systems
- ISO 20022
- FISMA – Federal Information Security Management Act of 2002

Minimum Security Controls

Security Control	Observations	Status	Content Type	Responsible Authority
Better and revised policies (M1)	Policies have been revised and are in full effect	Complete	Common	CIO
Stronger GRC approach (M2)	The Governance, Risk and Compliance sections are revised regularly.	Complete	Common	CIO
Separation of responsibilities and duties (M3)	Duties of all employees and management have been separated	Partial	Common	CIO
Meetings between various departments in the agency to discuss policies (M4)	Quarterly meetings are being conducted between departments	Complete	Common	CEO
Compliance Audits (M5)	Compliance audits are carried out on a regular basis	Complete	Common	CIO
Security awareness workshops and training (M6)	Security training and awareness workshops are carried out.	Partial	Common	CIO
Better Incident reporting and incident handling strategies (M7)	Incident reporting and handling procedures are being developed and updated regularly	Partial	Common	CIO
Incident response playbook (M8)	Incident response playbook created and updated regularly	Complete	Common	CISO
Planning for Backups and Reinitiating of Agency (M9)	Process for backups have been automated	Complete	Common	CISO
Physical Security (M10)	Physical Security measures have been implemented	Partial	Common	CISO
Managing and updating Audit logs and trails (M11)	SIEM systems have been successfully installed for auditing and logging.	Partial	Common	CISO
Better Access control policies (M12)	Improved access control policies have been implemented	Complete	Common	CIO
Stronger approach on data privacy and backup (M13)	Data privacy and data backup policies have been implemented	Complete	Common	CIO
Stronger and Better Authentication mechanisms (M14)	Improved authentication mechanisms have been implemented	Complete	Common	CISO

Information Security Plan Complete Date: 09/30/2022

Information Security Plan Approval Date: 10/04/2022

Information Assets Inventory:

ASSETS NO.	ASSET NAME	ASSET DESCRIPTION	ASSET VALUE
A1	Personal Computers [PC]	Computer Systems are used in the various departments of HGA.	\$450,000
A2	Financial Resources	HGA issues Paychecks and this is the most important asset.	\$1,000,000
A3	Business Documents	Includes all procedural documents, reports, memos, etc.	\$100,000
A4	Consoles	Provides certain special privileges to the administrative departments.	\$5,000
A5	Printers	Connected to all the PCs through LAN to generate Printing capabilities.	\$5,000
A6	Hard-Disk Drives	All PCs are installed with Hard-Disk Drives of different sizes depending on the use of the authorized personnel	\$80,000
A7	Routers	Network interfaces are installed around the organization that provides access to the internet.	\$16,000
A8	LAN Server	An intermediary server between the personal computers and the LAN.	\$15,000
A9	WAN Connection	Network connection that enables HGA to connection to other departments and other Agencies administered by the government.	\$13,000
A10	LAN	All data and information are shared using LAN between all the PCs.	\$7,000
A11	Email Server	In charge of storing, sending, and receiving emails within HGA and the internet.	\$6,000
A12	Personally Identifiable Information (PII)	Consists of employee data that can be linked to the employee directly like names, emails, addresses, etc.	\$500,000
A13	Reputation and Employee Confidence	This is the reputation HGA has in the industry and the confidence it's employees have on it	-

Subset of Assets:

ASSETS NO.	ASSET NAME	ASSET DESCRIPTION	ASSET VALUE
A1	Personal Computers [PC]	Computer Systems are used in the various departments of HGA.	\$450,000
A2	Financial Resources	HGA issues Paychecks and this is the most important asset.	\$1,000,000
A4	Consoles	Provides certain special privileges to the administrative departments.	\$5,000
A7	Routers	Network interfaces are installed around the organization that provides access to the internet.	\$16,000

List of Threats:

THREAT NO.	Threat
T1	Payroll Fraud
T2	Payroll errors
T3	Interruption of Operations
T4	Natural Disaster
T5	Unauthorized Access of services and assets
T6	Insider Threat
T7	Information theft
T8	Disclosure or brokerage of important information
T9	Disruption or misuse of System processes

Subset of Threats:

THREAT NO.	Threat
T1	Payroll Fraud
T2	Payroll errors
T5	Unauthorized Access of services and assets
T8	Disclosure or brokerage of important information

List Of Vulnerabilities:

VULNERABILITY NO.	VULNERABILITY
V1	Falsified Time Sheets
V2	Outdated passwords
V3	Unauthorized access to confidential information
V4	Corruption of data
V5	Loss of data
V6	Deletion of critical data
V7	Access to master database
V8	Unencrypted servers
V9	Unauthorized modification of critical data
V10	Lack of security policies

Subset of Vulnerabilities:

VULNERABILITY NO.	VULNERABILITY
V1	Falsified Time Sheets
V3	Unauthorized access to confidential information
V6	Deletion of critical data
V10	Lack of security policies

Threat-Vulnerability pairs with probabilities on Asset subset – A1, A2, A4, and A7

	T1	T2	T5	T8
V1	95	95	90	80
V3	90	95	85	90
V6	90	80	90	90
V10	95	85	90	90

Asset-Vulnerability Pairs:

Asset	Vulnerability No	Vulnerability
A1: Personal Computer [PC]	V3	Unauthorized access to confidential information
	V6	Deletion of critical data
A2: Financial Resources	V1	Falsified Time Sheets
	V6	Deletion of critical data
A4: Consoles	V6	Deletion of critical data
	V10	Lack of security policies
A7: Routers	V3	Unauthorized access to confidential information
	V6	Deletion of critical data
	V10	Lack of security policies

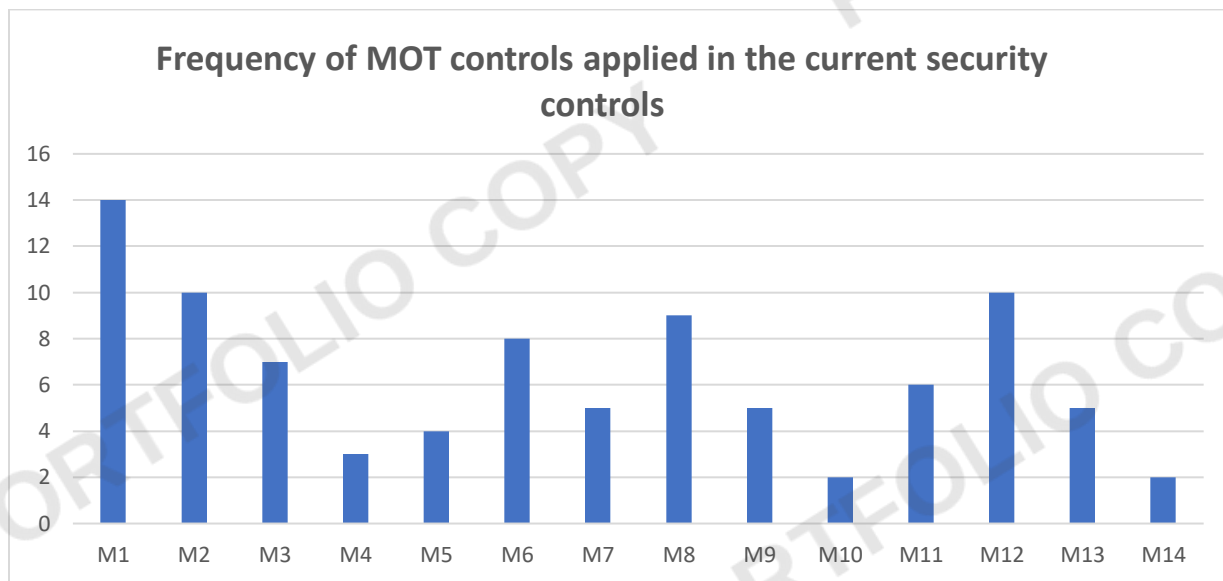
MOT controls:

Management	Operational	Technical
Better and revised policies (M1)	Security awareness workshops and training (M6)	Managing and updating Audit logs and trails (M11)
Stronger GRC approach (M2)	Better Incident reporting and incident handling strategies (M7)	Better Access control policies (M12)
Separation of responsibilities and duties (M3)	Incident response playbook (M8)	Stronger approach on data privacy and backup (M13)
Meetings between various departments in the agency to discuss policies (M4)	Planning for Backups and Reinitiating of Agency (M9)	Stronger and Better Authentication mechanisms (M14)
Compliance Audits (M5)	Physical Security (M10)	

Current Security Controls & Policies:

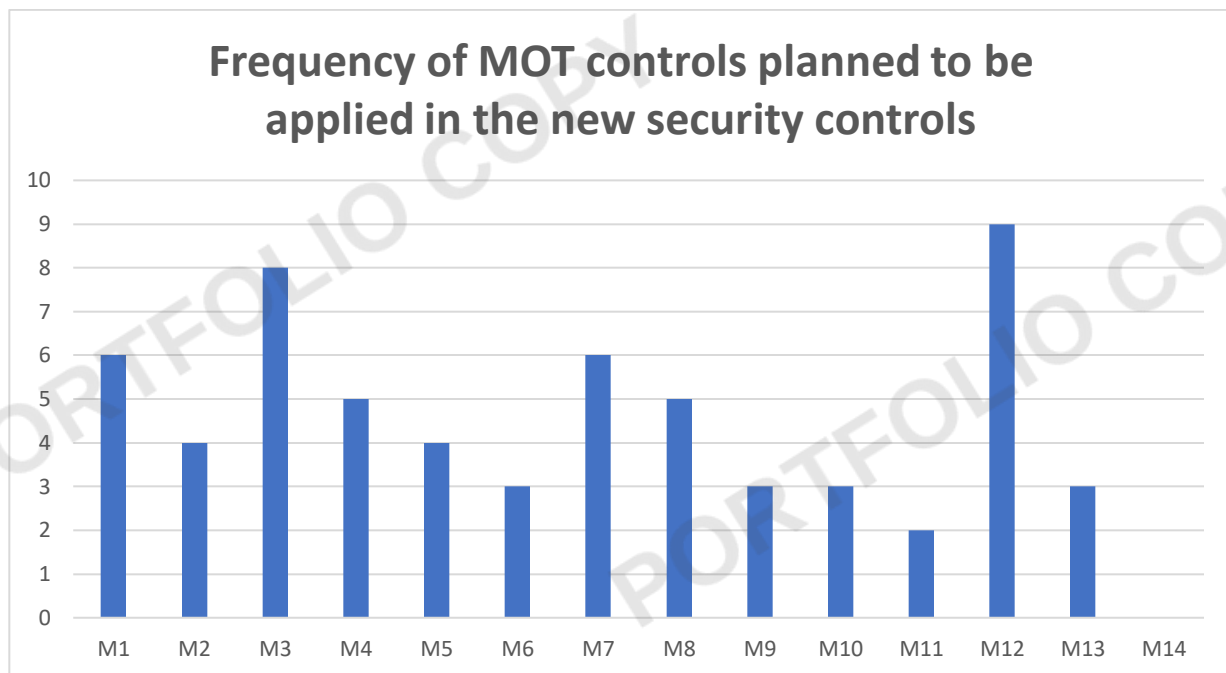
Current Security Controls & Policy No. (CSCP)	Security Control and Policy Description	M-O-T Controls
Payroll Fraud & errors		
CSCP1	Compliance of data according to the privacy act.	1,2,3,5,7,8,9,10,11,13
CSCP2	Identification and Authentication (I&A).	2,8,13
CSCP3	Protection against payroll errors.	1,3,5,6,8,13
CSCP4	Safeguard against Accidental corruption/loss of data.	3,6,7,8,12
CSCP5	Protection against unauthorized Execution of time and attendance application.	2,6,8,12,14
Network threats		

CSCP6	Rules for filtering packets	1,3,7,13
CSCP7	Denial Of Service attacks	2,5,6,8,9,11,13
CSCP8	Restrictions related to the router	1,9,10,12
Disclosure of information		
CSCP9	Need-to-know policy	1,2,6
CSCP10	Training and workshops on security awareness	2,6,12
CSCP11	Efficient Access control mechanisms	1,2,3,7,12
General Use and Administration of HGA's Computer System		
CSCP12	Compliance with HGA's general security and password protection policies.	1,2,6,8,12,14
CSCP13	Maintenance and administrative tasks are managed by Computer Operations Group (COG)	1,2,11
CSCP14	Security awareness training sessions and workshops	1,6,7,12
CSCP15	Strict Policies that imply authorization for sensitive data	1,5,8,12
Interruption of Operations		
CSCP16	Contingency Planning	1,2,9,11
CSCP17	Division Contingency Planning	1,4,9,11,12
Non-HGA Computer Systems		
CSCP18	Issue specific policy on the use of Internet	1,3,4,
CSCP19	No transmission policy of HGA's Proprietary data	1,3,4,8,11,12



New Security Controls & Policies:

New Security Controls & Policy No. (NSP)	Security Control and Policy Description	M-O-T Controls
Payroll Fraud & errors		
NSP1	Limiting access to payroll data	1,3,7,9,12
NSP2	Complying and reviewing security audit report	5,7,8,11,12
NSP3	Better Authentication using OTP (one-time passwords) and Multifactor Authentication	1,3,4,7,11,12
NSP4	Use of Digital Signatures	2,8,9,12,13
NSP5	Procedures for server administration	3,4, 8,12
Network threats		
NSP6	Stronger I/A	2,3,7,13
NSP7	Encryption of Modem	1,4,7,10
NSP8	Encryption of Mainframe communications	2,3,5,6,8,10
Continuity of Operations		
NSP9	Regular automatic backups	1,3,6,9,12
NSP10	Following a playbook	3,6,8,12
Disclosure of information		
NSP11	Need-to-know policy	1,4,7,10
NSP12	Training and workshops on security awareness	2,4,7,12
NSP13	Efficient Access control mechanisms	1,3,6,7,8,12,13



Security Risk Prevention Strategy

Threat-Vulnerability pairs with probabilities on Asset subset – A1, A2, A4, A7, A13 and A14

	T1	T2	T5	T8	T9
V1	10	15	5	5	10
V3	5	4	15	10	5
V6	5	5	4	5	15
V9	15	15	5	10	10
V10	5	5	10	5	10

Total risk = 208

Initial Risk Impacts: For worst case scenario when system resilience is 0%

	Threat X Vulnerability – Threat exploiting the vulnerability															
Assets	T1xV1	T1xV3	T1xV6	T1xV10	T2xV1	T2xV3	T2xV6	T2xV10	T5xV1	T5xV3	T5xV6	T5xV10	T8xV1	T8xV3	T8xV6	T8xV10
A1	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A2	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A4	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A7	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A13	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A14	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Therefore, Residual Security Risk = Asset Value x Total Threat

Residual Asset Security Risks:

1. Risk of A1= \$450,000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 15+ 15+ 5+ 10+ 10+ 5+ 5+ 10+ 5+ 10)= 450,000*208 = \$93,600,000> \$450,000
Therefore, Total Asset Loss
2. Risk of A2 = \$1,000,000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 15+ 15+ 5+ 10+ 10+ 5+ 5+ 10+ 5+ 10)= 1,000,000*208 = \$208,000,000 > \$1,000,000
Therefore, Total Asset loss.
3. Risk of A4 = \$5,000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 15+ 15+ 5+ 10+ 10+ 5+ 5+ 10+ 5+ 10)= 5,000*208 = \$1,040,000> \$5,000
Therefore, Total Asset Loss
4. Risk of A7: \$16000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 15+ 15+ 5+ 10+ 10+ 5+ 5+ 10+ 5+ 10)= 16,000*208 = \$3,328,000> \$16,000
Therefore, Total Asset Loss
5. Risk of A13: \$20000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 15+ 15+ 5+ 10+ 10+ 5+ 5+ 10+ 5+ 10)= 20,000*208 = \$4,160,000> \$20,000
Therefore, Total Asset Loss

6. Risk of A14: $\$6000 * (10 + 15 + 5 + 5 + 10 + 5 + 4 + 15 + 10 + 5 + 5 + 5 + 4 + 5 + 15 + 15 + 15 + 5 + 10 + 10 + 5 + 5 + 10 + 5 + 10) = 6,000 * 208 = \$1,248,000 > \$6,000$
Therefore, Total Asset Loss

- Residual Asset Vulnerability Risks

1. Risk due to V1:
 $\$ [(450,000 * 45) + (1,000,000 * 45) + (5,000 * 45) + (16000 * 45) + (20000 * 45) + (6000 * 45)] = \$67,365,000$
2. Risk due to V3:
 $\$ [(450,000 * 39) + (1,000,000 * 39) + (5,000 * 39) + (16000 * 39) + (20000 * 39) + (6000 * 39)] = \$58,383,000$
3. Risk due to V6:
 $\$ [(450,000 * 34) + (1,000,000 * 34) + (5,000 * 34) + (16000 * 34) + (20000 * 34) + (6000 * 34)] = \$50,898,000$
4. Risk due to V9:
 $\$ [(450,000 * 55) + (1,000,000 * 55) + (5,000 * 55) + (16000 * 55) + (20000 * 55) + (6000 * 55)] = \$82,335,000$
5. Risk due to V10:
 $\$ [(450,000 * 35) + (1,000,000 * 35) + (5,000 * 35) + (16000 * 35) + (20000 * 35) + (6000 * 35)] = \$52,395,000$

- Ranking of security asset residual risks:

Asset	Residual Security Risk	Rank
A2: Financial Resources	\$208,000,000	1
A1: Personal Computers	\$93,600,000	2
A13: DMZ	\$4,160,000	3
A7: Routers	\$3,328,000	4
A14: VPN Servers	\$1,248,000	5
A4: Consoles	\$1,040,000	6

- Ranking of vulnerability security risks:

Vulnerability	Vulnerability Security risks	Rank
V9: Unauthorized modification of critical data	\$82,335,000	1
V1: Falsified Time Sheets	\$67,365,000	2
V3: Unauthorized access to confidential information	\$58,383,000	3
V10: Lack of security policies	\$52,395,000	4
V6: Deletion of critical data	\$50,898,000	5

Security Risk Prevention Strategy Step P2: Apply additional Hardening Controls to the highest ranked Vulnerability Risk, with further reduced probabilities, thus further reducing the overall security asset residual risk and creating a new ranking of vulnerability security risks.

The above table displays the ranking of vulnerability security risks according to which vulnerability **V9: Unauthorized modification of critical data** is the highest ranked vulnerability. HGA does not have complete control of this particular vulnerability, but it is heavily applying access control policies and implementing secure sign-on functionalities that will reduce the impact of this vulnerability, as it is very important to maintain the integrity of critical data in HGA. Being an organization that deals with a lot of financial handling, if any authenticated user gets into the system and modifies critical data, it can be catastrophic for HGA. Enabling MFA (multi-factor authentication) and implementing stronger password policies is a good start to reducing the scale of such vulnerabilities.

Threat-Vulnerability pairs with probabilities on Asset subset – A1, A2, A4, A7, A13 and A14

	T1	T2	T5	T8	T9
V1	10	15	5	5	10
V3	5	4	15	10	5
V6	5	5	4	5	15
V9	5	5	5	4	5
V10	5	5	10	5	10

Total threat = 177

Initial Risk Impacts: For worst case scenario when system resilience is 0%

	Threat X Vulnerability – Threat exploiting the vulnerability															
Assets	T1xV1	T1xV3	T1xV6	T1xV10	T2xV1	T2xV3	T2xV6	T2xV10	T5xV1	T5xV3	T5xV6	T5xV10	T8xV1	T8xV3	T8xV6	T8xV10
A1	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A2	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A4	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A7	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A13	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A14	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Therefore, Residual Security Risk = Asset Value x Total Threat

Residual Asset Security Risks:

1. Risk of A1= \$450,000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 5+ 5+ 5+ 4+ 5+ 5+ 5+ 10+ 5+ 10) = 450,000*177 = \$79,650,000> \$450,000
Therefore, Total Asset Loss
1. Risk of A2 = \$1,000,000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 5+ 5+ 5+ 4+ 5+ 5+ 5+ 10+ 5+ 10) = 1,000,000*177 = \$177,000,000 > \$1,000,000
Therefore, Total Asset loss.

2. Risk of A4 = \$5,000(10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 5+ 5+ 5+ 4+ 5+ 5+ 5+ 10+ 5+ 10) = 5,000*177 = \$885,000 > \$5,000
Therefore, Total Asset Loss
3. Risk of A7: \$16000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 5+ 5+ 5+ 4+ 5+ 5+ 5+ 10+ 5+ 10) = 16,000*177 = \$2,832,000 > \$16,000
Therefore, Total Asset Loss
4. Risk of A13: \$20000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 5+ 5+ 5+ 4+ 5+ 5+ 5+ 10+ 5+ 10) = 20,000*177 = \$3,540,000 > \$20,000
Therefore, Total Asset Loss
5. Risk of A14: \$6000* (10+ 15+ 5+ 5+ 10 + 5+ 4+ 15+ 10+ 5+ 5+5+ 4+ 5+ 15+ 15+ 15+ 5+ 10+ 10+ 5+ 5+ 10+ 5+ 10) = 6,000*177 = \$1,062,000 > \$6,000
Therefore, Total Asset Loss

- Residual Asset Vulnerability Risks

1. Risk due to V1:
\$ [(450,000* 45) +(1,000,000* 45) +(5,000*45) +(16000*45) + (20000*45) + (6000*45)] = \$67,365,000
2. Risk due to V3:
\$ [(450,000* 39) +(1,000,000* 39) +(5,000*39) +(16000*39) + (20000*39) + (6000*39)] = \$58,383,000
3. Risk due to V6:
\$ [(450,000* 34) +(1,000,000* 34) +(5,000*34) +(16000*34) + (20000*34) + (6000*34)] = \$50,898,000
4. Risk due to V9:
\$ [(450,000* 24) +(1,000,000* 24) +(5,000*24) +(16000*24) + (20000*24) + (6000*24)] = \$35,928,000
5. Risk due to V10:
\$ [(450,000* 35) +(1,000,000* 35) +(5,000*35) +(16000*35) + (20000*35) + (6000*35)] = \$52,395,000

- Ranking of security asset residual risks:

Asset	Residual Security Risk	Rank
A2: Financial Resources	\$177,000,000	1
A1: Personal Computers	\$79,650,000	2
A13: DMZ	\$3,540,000	3
A7: Routers	\$2,832,000	4
A14: VPN Servers	\$1,062,000	5
A4: Consoles	\$885,000	6

- Ranking of vulnerability security risks:

Vulnerability	Vulnerability Security risks	Rank
V1: Falsified Time Sheets	\$67,365,000	1
V3: Unauthorized access to confidential information	\$58,383,000	2
V10: Lack of security policies	\$52,395,000	3
V6: Deletion of critical data	\$50,898,000	4
V9: Unauthorized modification of critical data	\$35,928,000	5

Security Risk Prevention Strategy Step P3: Apply additional Hardening Controls to the new, now highest-ranked Vulnerability Risk, thus further reducing the security asset residual risks and create a new ranking of vulnerability security risks.

The above table displays the ranking of vulnerability security risks according to which vulnerability **V1: Falsified Time Sheets** is the highest. HGA deals with a lot of financial data and having falsified time sheets is not only unsafe but also unprofitable for HGA.

It is a critical vulnerability as security policies make a company comply with the Governance, Risks and Compliance. Having a Lack of good security policies does not affect a single department or two but the entire HGA altogether. HGA should follow NIST cybersecurity guidelines and security architecture like other government agencies. Doing so will enable HGA to be more secure and eventually bring down the risk% for all vulnerabilities in HGA significantly.

Threat-Vulnerability pairs with probabilities on Asset subset – A1, A2, A4, A7, A13 and A14

	T1	T2	T5	T8	T9
V1	5	5	4	3	4
V3	5	4	15	10	5
V6	5	5	4	5	15
V9	5	5	5	4	5
V10	5	5	10	5	10

Total Threat: 153

Initial Risk Impacts: For worst case scenario when system resilience is 0%

Threat X Vulnerability – Threat exploiting the vulnerability																
Assets	T1xV1	T1xV3	T1xV6	T1xV10	T2xV1	T2xV3	T2xV6	T2xV10	T5xV1	T5xV3	T5xV6	T5xV10	T8xV1	T8xV3	T8xV6	T8xV10
A1	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A2	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A4	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A7	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A13	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A14	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Therefore, Residual Security Risk = Asset Value x Total Threat

Residual Asset Security Risks:

1. Risk of A1= \$450,000*
(5+5+4+3+4+5+4+15+10+5+5+5+4+5+15+5+5+5+4+5+5+5+10+5+10)= 450,000*153 =
\$68,850,000 > \$450,000
Therefore, Total Asset Loss
2. Risk of A2 = \$1,000,000*
(5+5+4+3+4+5+4+15+10+5+5+5+4+5+15+5+5+5+4+5+5+5+10+5+10)= 1,000,000*153 =
\$15,300,000 > \$1,000,000
Therefore, Total Asset loss.
3. Risk of A4 = \$5,000(5+5+4+3+4+5+4+15+10+5+5+5+4+5+15+5+5+5+4+5+5+5+10+5+10) =
5,000*153 = \$765,000 > \$5,000
Therefore, Total Asset Loss
4. Risk of A7: \$16000* (5+5+4+3+4+5+4+15+10+5+5+5+4+5+15+5+5+5+4+5+5+5+10+5+10)=
16,000*153 = \$2,448,000 > \$16,000
Therefore, Total Asset Loss
5. Risk of A13: \$20000* (5+5+4+3+4+5+4+15+10+5+5+5+4+5+15+5+5+5+4+5+5+5+10+5+10)=
20,000*153 = \$3,060,000 > \$20,000
Therefore, Total Asset Loss
6. Risk of A14: \$6000* (5+5+4+3+4+5+4+15+10+5+5+5+4+5+15+5+5+5+4+5+5+5+10+5+10) =
6,000*153 = \$918,000 > \$6,000
Therefore, Total Asset Loss

- Residual Asset Vulnerability Risks

1. Risk due to V1:
\$ [(450,000* 21) +(1,000,000* 21) +(5,000* 21) +(16000* 21) + (20000* 21) + (6000* 21)] =
\$31,437,000
2. Risk due to V3:
\$ [(450,000* 39) +(1,000,000* 39) +(5,000*39) +(16000*39) + (20000*39) + (6000*39)] = \$58,383,000
3. Risk due to V6:
\$ [(450,000* 34) +(1,000,000* 34) +(5,000*34) +(16000*34) + (20000*34) + (6000*34)] = \$50,898,000
4. Risk due to V9:
\$ [(450,000* 24) +(1,000,000* 24) +(5,000*24) +(16000*24) + (20000*24) + (6000*24)] = \$35,928,000
5. Risk due to V10:
\$ [(450,000* 35) +(1,000,000* 35) +(5,000*35) +(16000*35) + (20000*35) + (6000*35)] = \$52,395,000

- Ranking of security asset residual risks:

Asset	Residual Security Risk	Rank
A2: Financial Resources	\$153,000,000	1
A1: Personal Computers	\$68,850,000	2
A13: DMZ	\$3,060,000	3
A7: Routers	\$2,448,000	4
A14: VPN Servers	\$918,000	5
A4: Consoles	\$765,000	6

- Ranking of vulnerability security risks:

Vulnerability	Vulnerability Security risks	Rank
V3: Unauthorized access to confidential information	\$58,383,000	1
V10: Lack of security policies	\$52,395,000	2
V6: Deletion of critical data	\$50,898,000	3
V9: Unauthorized modification of critical data	\$35,928,000	4
V1: Falsified Time Sheets	\$31,437,000	5

Compare the list of current HGA controls plus CISO proposed response controls plus missing MOT response controls plus VPN plus DMZ risk controls to the 157 risk controls from Common Criteria.

HGA's recommendations have covered a lot of different security aspects; however, not all the policies of the MOT Model have been implemented. Under management controls, HGA has quite a lot of policies in effect, such as the adaptation of better and revised policies as well as the separation of responsibilities and duties throughout HGA, etc. Under operation controls, HGA has proposed to plan for backups and reinitiating of the agency as well as come up with better incident reporting and incident handling strategies. As for the technical controls that HGA has suggested, they will take a stronger approach on data privacy and backup and implement more robust and better authentication mechanisms. VPN was brought into HGA as a replacement for the current modem as a more secure alternative. The vpn server was integrated within the organization and has been a part of the internal network of HGA. Limiting VPN access should be the first step in securing the VPN server even more. Another safe practice to implement would be to block access to management interfaces through a VPN in case there is credential theft from an employee in a management position. Using strong cryptography policies and methods on the VPN server will not only help with the communication and data transactions through VPN but also make the VPN server more robust as a whole. The DMZ is a zone that must always be assumed to be insecure because it is a semi-trusted zone. Having a separate zone is better as it isolates data and makes the attack scale smaller through a network, but this only work efftetely if all the communication to and from the DMZ is encrypted correctly. Stronger policies must be implemented that restrict internal users of HGA from accessing the DMZ. Adding a dedicated firewall to tighten the communication between different zones and the DMZ can help secure the DMZ more. Continuous mentoring of communications and logs is a must when it comes to DMZ, and this will help HGA a lot in the long run.

Security Risk Response (Resilience) Strategy

Security Risk Response (Resilience) Strategy Step R1: Start with the results derived in Step P3 above. Keep threat/vulnerability pairs with probabilities as calculated in Step P3. Then calculate updated Residual Risk Rankings and Vulnerability Risk Rankings due to reducing risk impacts to less than 100% based on to implementing M-O-T controls which reduce risk impacts, without though negatively impacting operational effectiveness.

Below are the M-O-T controls, that I believe, would further reduce the risks associated with HGA's assets:

Management	Operational	Technical
Revised policies	Security awareness workshops and training	Managing and updating Audit logs and trails
Stronger GRC approach	Better Incident reporting and incident handling strategies	Better Access control policies
Separation of responsibilities and duties	Incident response playbook	Stronger approach on data privacy and backup

Threat-vulnerability pairs for vulnerabilities on asset subset: A1, A2, A4, A7, A13 and A14 after implementing the above controls.

	T1	T2	T5	T8	T9
V1	5	7	6	8	5
V3	5	6	6	7	5
V6	6	5	5	6	6
V9	5	5	5	4	5
V10	5	5	4	5	4

Updated Risk Impacts:

	Threat X Vulnerability – Threat exploiting the vulnerability														
Assets	T1xV1	T1xV3	T1xV6	T1xV9	T1xV10	T2xV1	T2xV3	T2xV6	T2xV9	T2xV10	T5xV1	T5xV3	T5xV6	T5xV9	T5xV10
A1	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A2	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A4	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A7	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A13	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A14	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%

Assets	T8xV1	T8xV3	T8xV6	T8xV10	T8xV1	T9xV1	T9xV3	T9xV6	T9xV9	T9xV10
A1	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A2	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A4	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A7	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A13	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A14	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%

Therefore, Residual Security Risk = Asset Value x Total Threat

Residual Asset Security Risks:

1. Risk of A1=

$$\$450,000 * (5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+4*50+5*50+5*50+4*50+5*50+4*50) = 450,000 * 6750 = \$303,750 > \$450,000$$

Therefore, Partial Asset Loss
2. Risk of A2 = \$1,000,000*

$$(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 1,000,000 * 6750 = \$675,000 > \$1,000,000$$

Therefore, Partial Asset loss.
3. Risk of A4 =

$$\$5,000(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 5,000 * 6750 = \$3,375 > \$5,000$$

Therefore, Partial Asset loss
4. Risk of A7: \$16000*

$$(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 16,000 * 6750 = \$10,800 > \$16,000$$

Therefore, Partial Asset loss
5. Risk of A13: \$20000*

$$(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 20,000 * 6750 = \$13,500 > \$20,000$$

Therefore, Partial Asset loss
6. Risk of A14: \$6000*

$$(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 6,000 * 6750 = \$4,050 > \$6,000$$

Therefore, Partial Asset loss

- Residual Asset Vulnerability Risks

1. Risk due to V1:

$$\$ [(450,000 * 31) + (1,000,000 * 31) + (5,000 * 31) + (16000 * 31) + (20000 * 31) + (6000 * 31)] = \$46,407,000$$
2. Risk due to V3:

$$\$ [(450,000 * 29) + (1,000,000 * 29) + (5,000 * 29) + (16000 * 29) + (20000 * 29) + (6000 * 29)] = \$43,413,000$$
3. Risk due to V6:

$$\$ [(450,000 * 28) + (1,000,000 * 28) + (5,000 * 28) + (16000 * 28) + (20000 * 28) + (6000 * 28)] = \$41,916,000$$
4. Risk due to V9:

$$\$ [(450,000 * 24) + (1,000,000 * 24) + (5,000 * 24) + (16000 * 24) + (20000 * 24) + (6000 * 24)] = \$35,928,000$$

5. Risk due to V10:

$$\$ [(450,000 * 23) + (1,000,000 * 23) + (5,000 * 23) + (16,000 * 23) + (20,000 * 23) + (6,000 * 23)] = \$34,431,000$$

- Ranking of security asset residual risks:

Asset	Residual Security Risk	Rank
A2: Financial Resources	\$675,000	1
A1: Personal Computers	\$303,750	2
A13: DMZ	\$13,500	3
A7: Routers	\$10,800	4
A14: VPN Servers	\$4,050	5
A4: Consoles	\$3,375	6

- Ranking of vulnerability security risks:

Vulnerability	Vulnerability Security risks	Rank
V1: Falsified Time Sheets	\$46,407,000	1
V3: Unauthorized access to confidential information	\$43,413,000	2
V6: Deletion of critical data	\$41,916,000	3
V9: Unauthorized modification of critical data	\$35,928,000	4
V10: Lack of security policies	\$34,431,000	5

Security Risk Response (Resilience) Strategy Step R2: Apply additional Hardening Controls (for example restricting services or adding a redundant server) to highest ranked Residual Asset Risk, thus further reducing risk impact probabilities, and further reducing the overall security asset residual risk and create a new ranking of vulnerability security risks. In this step you may need to include in the Asset inventory the value of points from the M-O-T Controls in Step R1 if the value of controls is comparable to value of Critical Assets.

From the given table about ranking of security asset residual risk of R1, we observed that asset A2: Financial resources is the highest-ranking asset. The overall risk of asset A2 can be reduced more significantly by implementing better authorization controls, regular backup of financial resources and isolation from other important data.

implementing the above controls.

	T1	T2	T5	T8	T9
V1	5	7	6	8	5
V3	5	6	6	7	5
V6	6	5	5	6	6
V9	5	5	5	4	5
V10	5	5	4	5	4

	Threat X Vulnerability – Threat exploiting the vulnerability														
Assets	T1xV1	T1xV3	T1xV6	T1xV9	T1xV10	T2xV1	T2xV3	T2xV6	T2xV9	T2xV10	T5xV1	T5xV3	T5xV6	T5xV9	T5xV10
A1	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A2	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%

A4	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A7	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A13	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A14	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%

Assets	T8xV1	T8xV3	T8xV6	T8xV10	T8xV1	T9xV1	T9xV3	T9xV6	T9xV9	T9xV10
A1	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A2	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A4	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A7	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A13	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A14	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%

Residual Asset Security Risks:

1. Risk of A1=
 $\$450,000 * (5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 450,000*6750 = \$303,750 > \$450,000$
Therefore, Partial Asset Loss
2. Risk of A2 = \$1,000,000*
 $(5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = 1,000,000*6750 = \$135,000 > \$1,000,000$
Therefore, Partial Asset loss.
3. Risk of A4 =
 $\$5,000(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 5,000*6750 = \$3,375 > \$5,000$
Therefore, Partial Asset loss
4. Risk of A7: \$16000*
 $(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 16,000*6750 = \$10,800 > \$16,000$
Therefore, Partial Asset loss
5. Risk of A13: \$20000*
 $(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 20,000*6750 = \$13,500 > \$20,000$
Therefore, Partial Asset loss
6. Risk of A14: \$6000*
 $(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = 6,000*6750 = \$4,050 > \$6,000$
Therefore, Partial Asset loss

- Residual Asset Vulnerability Risks

1. Risk due to V1:

$$\text{\$ } [(450,000 * 31 * 50) + (1,000,000 * 31 * 10) + (5,000 * 31 * 50) + (16000 * 31 * 50) + (20000 * 31 * 50) + (6000 * 31 * 50)] = \text{\$ } 10,803,500$$

2. Risk due to V3:

$$\text{\$ } [(450,000 * 29 * 50) + (1,000,000 * 29 * 10) + (5,000 * 29 * 50) + (16000 * 29 * 50) + (20000 * 29 * 50) + (6000 * 29 * 50)] = \text{\$ } 10,106,500$$

3. Risk due to V6:

$$\text{\$ } [(450,000 * 28 * 50) + (1,000,000 * 28 * 10) + (5,000 * 28 * 50) + (16000 * 28 * 50) + (20000 * 28 * 50) + (6000 * 28 * 50)] = \text{\$ } 9,758,000$$

4. Risk due to V9:

$$\text{\$ } [(450,000 * 24 * 50) + (1,000,000 * 24 * 10) + (5,000 * 24 * 50) + (16000 * 24 * 50) + (20000 * 24 * 50) + (6000 * 24 * 50)] = \text{\$ } 8,364,000$$

5. Risk due to V10:

$$\text{\$ } [(450,000 * 23 * 50) + (1,000,000 * 23 * 10) + (5,000 * 23 * 50) + (16000 * 23 * 50) + (20000 * 23 * 50) + (6000 * 23 * 50)] = \text{\$ } 8,015,500$$

- Ranking of security asset residual risks:

Asset	Residual Security Risk	Rank
A1: Personal Computers	\$303,750	1
A2: Financial Resources	\$135,000	2
A13: DMZ	\$13,500	3
A7: Routers	\$10,800	4
A14: VPN Servers	\$4,050	5
A4: Consoles	\$3,375	6

- Ranking of vulnerability security risks:

Vulnerability	Vulnerability Security risks	Rank
V1: Falsified Time Sheets	\$1,080,350	1
V3: Unauthorized access to confidential information	\$1,010,650	2
V6: Deletion of critical data	\$975,800	3
V9: Unauthorized modification of critical data	\$836,4000	4
V10: Lack of security policies	\$801,550	5

Security Risk Response (Resilience) Strategy Step R3: Apply additional Hardening Controls to new now highest ranked Residual Asset Risk, thus reducing risk impact probabilities, and further reducing the overall security asset residual risk and create a new ranking of vulnerability security risks. In this step you may need to include in the Asset inventory the value of points from the M-O-T Controls in Step R2 if the value of controls is comparable to value of Critical Assets.

After carefully observing the table from R2: Asset **A1: Personal Computers** have the highest residual security risk, and this risk can be significantly reduced by introducing better security policies to mitigate a lot of errors that might occur. Another policy that can be implemented is that to access these consoles you have to be locally connected to the network or connected via a VPN through and HGA's computer. Including an IDA (Intrusion Detection System) will go a long way with consoles as alarming the various departments about this will be a smart decision and can help the incident response team take required steps quicker.

After implementing the above controls on A1, A2, A4, A7, A13 and A14:

	T1	T2	T5	T8	T9
V1	5	7	6	8	5
V3	5	6	6	7	5
V6	6	5	5	6	6
V9	5	5	5	4	5
V10	5	5	4	5	4

Threat X Vulnerability – Threat exploiting the vulnerability															
Assets	T1xV1	T1xV3	T1xV6	T1xV9	T1xV10	T2xV1	T2xV3	T2xV6	T2xV9	T2xV10	T5xV1	T5xV3	T5xV6	T5xV9	T5xV10
A1	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A2	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A4	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A7	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A13	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A14	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%

Assets	T8xV1	T8xV3	T8xV6	T8xV10	T8xV1	T9xV1	T9xV3	T9xV6	T9xV9	T9xV10
A1	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A2	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A4	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A7	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A13	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%
A14	50%	50%	50%	50%	50%	50%	50%	50%	50%	50%

Residual Asset Security Risks:

1. Risk of A1=

$\$450,000 * (5*10 + 7*10 + 6*10 + 8*10 + 5*10 + 5*10 + 6*10 + 6*10 + 7*10 + 5*10 + 6*10 + 5*10 + 5*10 + 6*10 + 5*10 + 5*10 + 5*10 + 4*10 + 5*10 + 5*10 + 4*10 + 5*10 + 4*10) = \$60,750 < \$450,000$
Therefore, Partial Asset Loss

2. Risk of A2 = \$1,000,000*
 $(5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = \$135,000 < \$1,000,000$
 Therefore, Partial Asset loss.
3. Risk of A4 =
 $\$5,000(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = \$3,375 < \$5,000$
 Therefore, Partial Asset loss
4. Risk of A7: \$16000*
 $(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = \$10,800 < \$16,000$
 Therefore, Partial Asset loss
5. Risk of A13: \$20000*
 $(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = \$13,500 < \$20,000$
 Therefore, Partial Asset loss
6. Risk of A14: \$6000*
 $(5*50+7*50+6*50+8*50+5*50+5*50+6*50+6*50+7*50+5*50+6*50+5*50+5*50+6*50+6*50+5*50+5*50+5*50+4*50+5*50+5*50+5*50+4*50+5*50+4*50) = \$4,050 < \$6,000$
 Therefore, Partial Asset loss.

- Residual Asset Vulnerability Risks

1. Risk due to V1:
 $\$ [(450,000* 31*10) + (1,000,000* 31*10) + (5,000*31*50) + (16000*31*50) + (20000*31*50) + (6000*31*50)] = \$5,223,500$
2. Risk due to V3:
 $\$ [(450,000* 29*10) + (1,000,000* 29*10) + (5,000*29*50) + (16000*29*50) + (20000*29*50) + (6000*29*50)] = \$4,886,500$
3. Risk due to V6:
 $\$ [(450,000* 28*10) + (1,000,000* 28*10) + (5,000*28*50) + (16000*28*50) + (20000*28*50) + (6000*28*50)] = \$471,800$
4. Risk due to V9:
 $\$ [(450,000* 24*10) + (1,000,000* 24*10) + (5,000*24*50) + (16000*24*50) + (20000*24*50) + (6000*24*50)] = \$404,400$
5. Risk due to V10:
 $\$ [(450,000* 23*10) + (1,000,000* 23*10) + (5,000*23*50) + (16000*23*50) + (20000*23*50) + (6000*23*50)] = \$387,550$

- Ranking of security asset residual risks:

Asset	Residual Security Risk	Rank
A2: Financial Resources	\$135,000	1
A1: Personal Computers	\$60,750	2
A13: DMZ	\$13,500	3
A7: Routers	\$10,800	4
A14: VPN Servers	\$4,050	5
A4: Consoles	\$3,375	6

- Ranking of vulnerability security risks:

Vulnerability	Vulnerability Security risks	Rank
V1: Falsified Time Sheets	\$5,223,500	1
V3: Unauthorized access to confidential information	\$4,886,500	2
V6: Deletion of critical data	\$471,800	3
V9: Unauthorized modification of critical data	\$404,400	4
V10: Lack of security policies	\$387,550	5

Compare the list of current HGA controls plus CISO proposed response controls plus missing MOT response controls plus VPN plus DMZ risk controls to the 157 risk controls from Common Criteria.

HGA's recommendations have covered a lot of different security aspects; however, not all the policies of the MOT Model have been implemented. Under management controls, HGA has quite a lot of policies in effect, such as the adaptation of better and revised policies as well as the separation of responsibilities and duties throughout HGA, etc. Under operation controls, HGA has proposed to plan for backups and reinitiating of the agency as well as come up with better incident reporting and incident handling strategies. As for the technical controls that HGA has suggested, they will take a stronger approach on data privacy and backup and implement more robust and better authentication mechanisms. VPN was brought into HGA as a replacement for the current modem as a more secure alternative. The VPN server was integrated within the organization and has been a part of the internal network of HGA. Limiting VPN access should be the first step in securing the VPN server even more. Another safe practice to implement would be to block access to management interfaces through a VPN in case there is credential theft from an employee in a management position. Using strong cryptography policies and methods on the VPN server will not only help with the communication and data transactions through VPN but also make the VPN server more robust as a whole. The DMZ is a zone that must always be assumed to be insecure because it is a semi-trusted zone. Having a separate zone is better as it isolates data and makes the attack scale smaller through a network, but this only work effectively if all the communication to and from the DMZ is encrypted correctly. Stronger policies must be implemented that restrict internal users of HGA from accessing the DMZ. Adding a dedicated firewall to tighten the communication between different zones and the DMZ can help secure the DMZ more. Continuous mentoring of communications and logs is a must when it comes to DMZ, and this will help HGA a lot in the long run. All common vulnerabilities and errors are to be identified by a team and mitigated. For errors that have a human element attached to them, security awareness and security training must be conducted through HGA, including the higher up and management. Time and effort should be focused on the necessary security requirements and contingency plans must be made. For both the VPN server as well as DMZ, there must be backups arranged so as to deal with a situation if either of these critical entities were effected and are unfunctional for even a smaller amount of time as the ROI on this for HGA would be a considerable amount.

MIXED: Security Risk Prevention Strategy and Security Risk Response (Resilience) Strategy

On combining both the preventive and responsive security control P3 and R3 we get a mixed strategy which significantly reduces the risk impacts. After implying all the above listed security controls, authorization controls, IDEs, and various other functionalities, better and reduced risks results can be obtained. A table below shows the reduced risk impacts after applying mixed strategies.

After implementing the above controls on A1, A2, A4, A7, A13 and A14:

	T1	T2	T5	T8	T9
V1	5	7	6	8	5
V3	5	6	6	7	5
V6	6	5	5	6	6
V9	5	5	5	4	5
V10	5	5	4	5	4

Total threat = 135

Threat X Vulnerability – Threat exploiting the vulnerability															
Assets	T1xV1	T1xV3	T1xV6	T1xV9	T1xV10	T2xV1	T2xV3	T2xV6	T2xV9	T2xV10	T5xV1	T5xV3	T5xV6	T5xV9	T5xV10
A1	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A2	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A4	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A7	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A13	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A14	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%

Assets	T8xV1	T8xV3	T8xV6	T8xV10	T8xV1	T9xV1	T9xV3	T9xV6	T9xV9	T9xV10
A1	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A2	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A4	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A7	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A13	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A14	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%

Residual Asset Security Risks:

1. Risk of A1=
 $\$450,000 * (5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = \$60,750 > \$450,000$
 Therefore, Partial Asset Loss
2. Risk of A2 = \$1,000,000*
 $(5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) =$

$5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = \$135,000 > \$1,000,000 =$
Therefore, Partial Asset loss.

3. Risk of A4 =

$\$5,000(5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = \$675 < \$5,000$

Therefore, Partial Asset loss

4. Risk of A7: \$16000*

$(5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = \$2,160 < \$16,000$

Therefore, Partial Asset loss

5. Risk of A13: \$20000*

$(5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = \$2,700 < \$20,000$

Therefore, Partial Asset loss

6. Risk of A14: \$6000*

$(5*10+7*10+6*10+8*10+5*10+5*10+6*10+6*10+7*10+5*10+6*10+5*10+5*10+6*10+6*10+5*10+5*10+5*10+4*10+5*10+5*10+5*10+4*10+5*10+4*10) = \$810 < \$6,000$

Therefore, Partial Asset loss.

- Residual Asset Vulnerability Risks

1. Risk due to V1:

$\$ [(450,000* 31*10) + (1,000,000* 31*10) + (5,000*31*10) + (16000*31*10) + (20000*31*10) + (6000*31*10)] = \$46,407$

2. Risk due to V3:

$\$ [(450,000* 29*10) + (1,000,000* 29*10) + (5,000*29*10) + (16000*29*10) + (20000*29*10) + (6000*29*10)] = \$43,413$

3. Risk due to V6:

$\$ [(450,000* 28*10) + (1,000,000* 28*10) + (5,000*28*10) + (16000*28*10) + (20000*28*10) + (6000*28*10)] = \$41,916$

4. Risk due to V9:

$\$ [(450,000* 24*10) + (1,000,000* 24*10) + (5,000*24*10) + (16000*24*10) + (20000*24*10) + (6000*24*10)] = \$35,928$

5. Risk due to V10:

$\$ [(450,000* 23*10) + (1,000,000* 23*10) + (5,000*23*10) + (16000*23*10) + (20000*23*10) + (6000*23*10)] = \$34,431$

- Ranking of security asset residual risks:

Asset	Residual Security Risk	Rank
A2: Financial Resources	\$135,000	1
A1: Personal Computers	\$60,750	2
A13: DMZ	\$2,700	3
A7: Routers	\$2,160	4
A14: VPN Servers	\$810	5
A4: Consoles	\$675	6

- Ranking of vulnerability security risks:

Vulnerability	Vulnerability Security risks	Rank
V1: Falsified Time Sheets	\$46,407	1
V3: Unauthorized access to confidential information	\$43,413	2
V6: Deletion of critical data	\$41,916	3
V9: Unauthorized modification of critical data	\$35,928	4
V10: Lack of security policies	\$34,431	5

Conclusion: Cost Benefit Analysis

Did the HGA team address all security risks based on your risk assessment for HGA?

HGA's risk management recommendations have implemented many management, operational and technical controls all over HGA and its technical assets. Many preventive and responsive strategies have been implemented and are in the process of being implemented to reduce the risks of all the threats and vulnerabilities that HGA has to deal with currently. They have mixed the preventive and response strategies into a mixed approach to creating the best possible plan that takes the best part from the above plans and makes the risk analysis and assessment optimal. The risk assessment of HGA seemed like a very informational, technical, and overall very comprehensive as they were able to identify most of the security risks their organization was dealing with.

The Management-Operational-Technical model was very effectively implemented by HGA. HGA's recommendations covered a lot of policies, though not all the policies of the M-O-T model. Under management controls, HGA has effectively revised a lot of the important policies while having a strong GRC approach and separating the responsibilities and duties of employees. Under operational controls, HGA has raised security awareness and conducted security training workshops for not only the employees of HGA but as well the higher-ups. They have also made incident reporting and incident handling strategies better than before while also updating their incident response playbook significantly. Under Technical controls, HGA has started to efficiently manage and update audit logs and trails and implemented much better technical control policies for HGA. They have also implemented a more robust approach on data privacy and backup. The above-mentioned controls are just a few of the many controls implemented by HGA.

Although HGA has done a great job with the security risks, there are a few risk factors that HGA must focus more on, such as Improved access control mechanisms and improved authentication mechanisms all around HGA. Implementing access controls will ensure the integrity and confidentiality of critical data, which is a must for HGA as it deals with many financial assets. Better authentication will consist of implementing stronger passwords, MFA (multifactor authentication), and addition OTPs. Using more robust encryption strategies will ensure confidentiality inside the communications of HGA, which can be a good game changer for the organization. HGA should revise its existing security policies regularly and keep updating them with the industry's new security and vulnerability trends. HGA is recommended to use SIEM (Security Information and Event Management) for centralizing the auditing and logging practices inside HGA for better Intrusion detection and accountability.

This Security Risk Assessment was performed to identify and mitigate risks associated with various assets of HGA and the vulnerabilities and threats attached to them. This was done by first Identifying all the dangers, Assets, and Vulnerabilities of HGA's system and calculating residual risks after applying risk prevention, response, and mixed strategies. HGA has also added MOT controls and new and revised security policies through the organization to its already existing security controls and procedures. Post-risk assessment, HGA needs to focus more on implementing the security controls that were recommended to them, such as the ones mentioned, and keep the security policies up-to-date to keep up with the changing security trends.

Do you recommend a Risk Prevention Strategy or a Risk Response Strategy or a combination of both?

Risk prevention strategies as well as Risk response strategies, are crucial in any organization that wants to protect its assets. Risk prevention strategies are those risk strategies that are more preventive in nature there put into effect before an incident occurs, whereas Risk response strategies are the controls or policies that are brought into effect when an incident is currently taking place or has already happened and is used to prevent it from causing more damage and scaling itself to other assets and architectures that might be present inside an organization.

I would always recommend a mixed strategy as it is best to implement strategies that are preventive in nature to be ready for a possible attack, and it is also better to have response strategies in case there. For instance, having a strong requirement for passwords is a good risk-prevention strategy for all users in an organization. Having stronger authentication like MFA is also a good risk prevention strategy; however, If credentials are stolen or a physical system that has critical data has gone missing, remote wipeout and denying of access to the system and account is a good risk response strategy. Both are important in their own ways and neither can be ignored for the other one as they both go hand-in-hand to provide better security ranking to any organization.

Does the residual risk reduction exceed the budget for proposed controls?

Controls Mitigation	Risk Prevention Budget	Risk Response Budget	Mixed Strategy Budget
Payroll Fraud	\$75,000	\$60,000	\$150,000
Payroll errors	\$75,000	\$55,000	\$135,000
Continuity of Operations	\$65,000	\$60,000	\$100,000
Disclosure or brokerage of important information	\$80,000	\$80,000	\$130,000
Network related attacks	\$35,000	\$60,000	\$120,000
Review of Security controls	\$65,000	\$70,000	\$80,000
VPN	\$20,000	\$15,000	\$30,000
DMZ	\$25,000	\$25,000	\$55,000
Total:	\$440,000	\$425,000	\$800,000

Residual Risk = Risk with current controls – Risk with new controls

$\$1,480,000 - \$300,000 = \$1,180,000$

In this case, the value of risk reduction exceeds the budget of the proposed controls.

Proposed security budget cost for 3 budgets:

- Cost Benefit ratio analysis for Risk Prevention Budget
Proposed Security Risk Budget Cost/ Expected security risk-benefit
 $\$440,000/\$1,180,000 = 0.372$
- Cost Benefit ratio analysis for Risk Response Budget
Proposed Security Risk Budget Cost/ Expected security risk-benefit
 $\$425,000/\$1,180,000 = 0.360$
- Cost Benefit ratio analysis for Mixed strategy Budget
Proposed Security Risk Budget Cost/ Expected security risk-benefit
 $\$800,000/\$1,180,000 = 0.677$

PART B : Security Risk Management Implementation Plan

A) Access Control Security Risk Management Implementation Controls and Policies

- Identification Credentials
- Personal Authentication
- Authorization
- Logical Access Control Methods
- Physical Access Control Methods
- Biometric Systems

List of Critical assets in \$ that exist in Autumn-CSTL

ASSET ID	ASSET NAME	ASSET VALUE IN USD
A1	Personally Identifiable Information	\$300,000
A2	Database system	\$450,000
A3	Network Devices and Infrastructure	\$230,000
A4	Financial resources	\$200,000
A5	Information System Devices	\$550,000
A6	Application software	\$350,000
A7	Reputation	Intangible
A8	Intellectual Property (IP)	\$500,000

List of Missing Cybersecurity Implementation Controls:

Missing Controls
Identification Credentials
SSN
Biometrics
Personal Authentication
Photograph
Biometric
Logical Access Control Methods
PKI Compliance policies
DoD Common Access Cards
Alternate Login Token
Physical Access Control Methods
Attended Access
Biometric Identification system
Biometrics Systems
Facial Reorganization system
Retina Scanners

List Of Potential Vulnerabilities

1. Weak Authentication
2. Unauthorized access
3. Weak Access Control
4. Information theft
5. Equipment failure
6. Social Engineering

List Of Potential Threats:

1. Loss of Integrity, Confidentiality, privacy
2. Disclosure of highly sensitive information
3. Loss of availability
4. Service disruption
5. Information theft

List Of Possible Risks:

1. Security Breach
2. Organization service interruption
3. Data privacy loss
4. Noncompliance fines
5. Unavailability of critical assets

B] Network Infrastructure Security Risk Management Implementation Controls and Policies

- Enclave Protection
- Firewalls
- Routers

List of critical assets in \$ that exists in Autumn-CSTL

ASSET ID	ASSET NAME	ASSET VALUE IN USD
A1	Personally Identifiable Information	\$300,000
A2	Database system	\$450,000
A3	Network Devices and Infrastructure	\$230,000
A4	Financial resources	\$200,000
A5	Information System Devices	\$550,000
A6	Application software	\$350,000
A7	Reputation	Intangible
A8	Intellectual Property (IP)	\$500,000

List of missing Cybersecurity Implementation Controls:

Missing Controls
Enclave Protection
Network Test Access Ports (TAP)
Wireless Intrusion Detection system (WIDS)
Firewalls
Bastion Host
Deep Packet Inspection Firewall
Proxy server
Hybrid Technology Firewall
Routers
Securing Router Planes

List Of Potential Vulnerabilities

1. Information Theft
2. Denial Of Service Attacks (DoS)
3. Unauthorized Access
4. Network Infrastructure attack
5. Application layer attack
6. Network Port Scan
7. Wireless Attack
8. Firewall misconfiguration
9. Weak Firewall Protection

List of Potential Threats:

1. Loss of confidentiality, Integrity, Privacy, availability
2. Information theft
3. unauthorized access
4. Interruption of operations
5. Sensitive information disclosure

List of Possible Risks

- Security Breach
- Interruption of Operations
- Malware attacks
- Data Privacy Loss
- Non-Compliance Issues and fines
- Unavailability of business-critical assets and services
- Failure to achieve business objective

C] Network Infrastructure Security Risk Management Implementation controls and policies

- Ports, Protocols, & Services
- Device Management
- Device Monitoring
- Network Authentication, Authorization, & Accounting
- Network Intrusion Detection Systems (NIDS)
- Switches & VLANs
- Virtual Private Network

List of critical assets in \$ that exists in Autumn-CSTL

ASSET ID	ASSET NAME	ASSET VALUE IN USD
A1	Personally Identifiable Information	\$300,000
A2	Database system	\$450,000
A3	Network Devices and Infrastructure	\$230,000
A4	Financial resources	\$200,000
A5	Information System Devices	\$550,000
A6	Application software	\$350,000
A7	Reputation	Intangible

A8	Intellectual Property (IP)	\$500,000
----	----------------------------	-----------

List of Missing Cybersecurity Controls:

Missing Controls
Ports, Protocols, & Services
IPv6 Address Filtering
Unicast Reverse Path Forwarding
Device Management
Vulnerability Management System
Out-of-Band Management
Switches & VLANs
VLAN Trunking
Port Security
Virtual Private Network
Host to Host

List of Potential Vulnerabilities

1. Information Theft
2. Man-in-the-Middle
3. Data Tampering
4. Data theft
5. Unauthorized Access
6. Network Port Scan
7. Malicious Network Attacks
8. Interruption of Operations
9. MAC Address Spoofing
10. Network Misconfigurations
11. Malware and Injection Attacks
12. Denial Of Service (DoS)
13. Network Infrastructure Attack
14. Unpatched/obsolete software
15. Compliance Violations
16. IP address Spoofing

List of Potential Threats

1. Loss of Confidentiality
2. Loss of Integrity
3. Loss of Availability
4. Loss of Data Privacy
5. Information Theft
6. Interruption of Operations
7. Unauthorized Access

List of Possible Risks

- Security Breach
- Interruption of Operations
- Man-in-the-middle Attacks.
- Denial Of Service Attacks
- Data Privacy Loss
- Unavailability of business-critical assets and services
- Non-Compliance Issues and Fines
- Failure to achieve business objective.

D] Database Security Risk Management Implementation Controls and Policies

- Authentication
- Authorization
- Confidentiality
- Data Integrity
- Auditing
- Replication and Federation
- Database Clustering
- Backup and Recovery
- Operating Systems Protection
- Application Protection
- Network Protections
- Security Design & Configuration
- Enclave and Computing Environment:
- Business Continuity
- Vulnerability & Incident Management

List of critical assets in \$ that exists in Autumn-CSTL

ASSET ID	ASSET NAME	ASSET VALUE IN USD
A1	Personally Identifiable Information	\$300,000
A2	Database system	\$450,000
A3	Network Devices and Infrastructure	\$230,000
A4	Financial resources	\$200,000
A5	Information System Devices	\$550,000
A6	Application software	\$350,000
A7	Reputation	Intangible
A8	Intellectual Property (IP)	\$500,000

List of missing Cybersecurity Implementation Controls:

Missing Controls
Authorization
Renaming Default Accounts
Network Protections
Limiting Network Session Parameters
Security Design & Configuration
Ports, Protocols, and services
Configuration Management Process
Key Management
Enclave and Computing Environment
Access for need to know
Software development change controls
Boundary defense
Business Continuity
Disaster & Recovery Plan

List of Potential Vulnerabilities:

1. Broken Access Control
2. Unauthorized Access
3. Disruption of Business
4. Loss of Data
5. Privilege Escalation
6. Dos Attack
7. Network Session Hijacking

List of Potential Threats:

- Loss of Confidentiality, Integrity, and Availability
- Loss of Data Privacy
- Information theft
- Interruption of Operations
- Unauthorized Access
- Non-Compliance Issues

List of Possible Risks:

- Data breach
- Interruption of Operations
- Non-Compliance Issues and fines
- Data privacy loss
- Denial-of-Service Attacks
- Malware Attacks on OS
- Failure to achieve Business Objective

E] Application Security Risk Management Implementation Controls and Policies

- Application Data Handling
- Authentication
- Cryptography
- User Accounts
- Input Validation
- Application Auditing
- Configuration Management
- Testing
- Deployment

List of critical assets in \$ that exists in Autumn-CSTL

ASSET ID	ASSET NAME	ASSET VALUE IN USD
A1	Personally Identifiable Information	\$300,000
A2	Database system	\$450,000
A3	Network Devices and Infrastructure	\$230,000
A4	Financial resources	\$200,000
A5	Information System Devices	\$550,000
A6	Application software	\$350,000
A7	Reputation	Intangible
A8	Intellectual Property (IP)	\$500,000

List of missing Cybersecurity Implmenetation Controls:

Missing Controls
Application Data Handling
Data Marking
Authentication
Signed Code Identification
Client Application Authentication
Cryptography
Digital Signature
User Accounts
Application Sessions
Input Validation
Input Sanitization
Prepared Statements
Testing
Automated Tools

List of Potential Vulnerabilities:

1. Unauthorized access
2. Unauthorized modification
3. Insecure code vulnerabilities
4. Information disclosures
5. Loss of integrity
6. System Failure
7. SQL injection
8. Information Theft

List of Potential Threats:

- Data theft
- Data tampering
- Unauthorized use or disclosure of sensitive information
- Data corruption
- System instability
- Malware injection
- Breach of confidentiality
- Loss of sensitive data
- Corruption or destruction of data
- Unauthorized data modification
- System downtime
- Inability to access critical systems
- Unauthorized data access
- Loss of confidential data
- Identity theft
- Financial loss.

List of Possible Risks:

- Information disclosure
- loss of integrity
- Insecure code vulnerabilities
- unauthorized code modification
- Unauthorized access
- SQL injection
- system failure.

F] Wireless Security Risk Management Implementation controls and Policies

- Wireless LAN Risk Management
- Wireless PAN Risk Management
- Wireless PAN Risk Management
- Wireless RFID Risk Management
- Wireless PED Risk Management

List of critical assets in \$ that exists in Autumn-CSTL

ASSET ID	ASSET NAME	ASSET VALUE IN USD
A1	Personally Identifiable Information	\$300,000
A2	Database system	\$450,000
A3	Network Devices and Infrastructure	\$230,000
A4	Financial resources	\$200,000
A5	Information System Devices	\$550,000
A6	Application software	\$350,000
A7	Reputation	Intangible
A8	Intellectual Property (IP)	\$500,000

List of Missing Cybersecurity Controls:

Missing Controls
Wireless LAN Risk Management
Protected Extensible Authentication Protocol (PEAP)
Security Boundary Implementations for DOD
Wireless PED Risk Management
PED Security

List of Potential Vulnerabilities:

1. Unauthorized access
2. Information Disclosures
3. Broken Authentication
4. Wireless Attacks
5. Unauthorized Modification

List of Potential Threats

- Loss of Confidentiality, Integrity, Privacy and availability
- Unauthorized access
- Information Disclosure
- Non-compliance issues
- System data corruption

List of Possible Risks:

- Data breach
- Data privacy and confidentiality loss
- Information theft
- Leaking of sensitive data
- Wireless network attacks

List of Cybersecurity Implementation controls present at Autumn-CSTL

A| Access Control Security Risk Management Implementation Controls and Policies

Cybersecurity implementation controls
Identification Credentials
Password
Digital Certificate
Photograph
Access Card
Employee ID card
Personal Authentication
Password
Digital certificate
Employee ID card
Access Card
Single Sign-on
Authorization
Access Control Lists
Security Policy
Tokens
Logical Access Control Methods
Encryption
Remote network access
Network architectural controls
Network Access Controls
Network Ports Security
Passwords
PINs
Physical Access Control Methods
Classified Storage and Handling
Badges
Smart cards
Physical tokens
PINs
Physical Intrusion Detection System
Biometrics Systems
Fingerprint Readers

B| Network Infrastructure Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls
Enclave Protection
Defense-in-Depth
Firewalls
Routers
Switches
Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)
Demilitarized Zone (DMZ)
VPN Tunnel
Firewalls
Packet Filtering Firewall
Stateful Inspection Firewall
Application Proxy Gateway
Routers
Route Table Integrity

C| Network Infrastructure Security Risk Management Implementation controls and policies

Cybersecurity Implementation Controls
Ports, Protocols, & Services
Classification of Ports
Restricting ICMPv4 Echo Request & Reply
Preventing Traceroute
IPv4 Address Filtering
Protecting Servers from SYN Flood Attacks
Device Management
Software Updates
In-Band Management
Device Monitoring
Simple Network Management Protocol
Network Management Station
Network Authentication, Authorization, & Accounting
Authentication
Authorization
Accounting
Auditing
Router Password Protecting
Network Intrusion Detection Systems (NIDS)
Local Area NIDS
External NIDS
Switches & VLANs
Physical Security
VLANs
801/1X & Management Policy Server
Virtual Private Network
Gateway to Gateway
Host to Gateway

D| Database Security Risk Management Implmentatoin Controls and Policies

Cybersecurity Implementation Controls
Authentication
User Account
Database Administrator (DBA)
Application Owner
Application User Manager
Application Account
Database Auditor
Database Operator
Passwords
Certificates
External Authentication
Credentials Storage
Authorization
Role Based Access Control (RBAC)
Confidentiality
Data Encryption
Application Code Encryption
Sensitive Data Encryption
Data Integrity
Data Integrity
Transaction Logs
Auditing
Audit Logs
Audit Logs Protection
Audit Logs Storage
Replication and Federation
Database Replication
Federated Database
Database Clustering
Database Clustering
Principle of Least Privilege
Accountability
Backup and Recovery
Testing and Maintenance

Backup Encryption
Backup Authentication & Authorization
Operating Systems Protection
Disk Partitions
Separation of Accounts
Database Software
Application Protection
Principle of least Privilege
Auditing Elevated Privileges
Input Validation
Application Authentication
Network Protections
Network Access
Encryption
Security Design & Configuration
Procedural Review
Configuration Specifications
Compliance Testing
Non- Repudiation
Partitioning of the application
IA Documentation
System library management controls
Security Structure support partitioning
System State Changes
Software Baseline
Group Identification and authentication
Individual Identification and authentication
Token and certificate standards
Enclave and Computing Environment
Audit Record content
Audit trail, monitoring, analysis, and reporting
Changes to data
Encryption for Confidentiality
Data change controls
Interconnections among systems and enclaves

Audit of security label changes
Logon
Least Privilege
Marking and labeling
Production code change controls
Resource Control
Audit reduction and report generation
Audit Record Retention
Security Configuration Compliance
Warning Messages
Business Continuity
Protection of backup & Restoration Assets
Data Backup Procedure
Backup of Critical Software
Trusted Recovery
Vulnerability & Incident Management
Vulnerability Management

E| Application Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls
Application Data Handling
Database Management System
Data Storage
In-Memory Data Handling
Data Transmission
Data Integrity
Authentication
Server Authentication
User Authentication
Standalone Application Authentication
Server Application Authentication
Combination Client Server Application Authentication
Application Component Authentication
Cryptography
Symmetric Ciphers
Message Authentication Code
User Accounts
User Accounts
Duplicate User Accounts
Account Lockout Policy
Access Controls

Input Validation
Input Validation
Static Analysis Tools
Remove Hidden Fields
Application Auditing
Audit Scope
Protecting Audit Trails
Configuration Mangement
Software Configuration Management
Limiting Unauthorized Modification
Testing
Test Plans & Procedures
Fuzzy Testing
Code Reviews
Deployment
Documentation
Auditing

F| Wireless Security Risk Management Implementation controls and Policies

Cybersecurity Implementation Controls
Wireless LAN Risk Management
IEEE 802.1x Extensible Authentication Protocol
EAP Transport Layer Security (EAP-TLS)
EAP Tunneling Transport Layer Security
WLAN Components
Access Point
Separation of Networks
Wi-fi Protected Access 2 (WPA2)
VPN
Access Point & Client Identification
Data-in-transit Encryption
Wireless PAN Risk Management
Bluetooth
Pairing/Bonding
Confidentiality
Integrity
Authentication
Authorization
Wireless PAN Risk Management
Cellular Digital Packet Data
Wireless RFID Risk Management
Radio Frequency Identification
Wireless PED Risk Management
Subscriber Identity Module
Wireless Two-Way Email

Compare the Implementation Controls with your company's Existing Cybersecurity Implementation Controls

A| Access Control Security Risk Management Implementation Controls and Policies

Cybersecurity implementation controls	Implementation status
Identification Credentials	
Password	Present
Digital Certificate	Present
SSN	Absent
Photograph	Present
Biometrics	Absent
Access Card	Present
Employee ID card	Present
Personal Authentication	
Password	Present
Digital certificate	Present
Employee ID card	Present
Photograph	Absent
Biometric	Absent
Private Key	Absent
Access Card	Present
Single Sign-on	Present
Authorization	
Access Control Lists	Present
Security Policy	Present
Tokens	Present
Logical Access Control Methods	
Encryption	Present
Remote network access	Present
Network architectural controls	Present
Network Access Controls	Present
Network Ports Security	Present
PKI Compliance policies	Absent
Passwords	Present
PINs	Present
DoD Common Access Cards	Absent
Alternate Login Token	Absent
Physical Access Control Methods	
Attended Access	Absent
Classified Storage and Handling	Present
Badges	Present
Biometric Identification system	Absent
Smart cards	Present
Physical tokens	Present
PINs	Present
Physical Intrusion Detection System	Present

Biometrics Systems	
Facial Reorganization system	Absent
Retina Scanners	Absent
Fingerprint Readers	Present

B] Network Infrastructure Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls	Implementation Controls
Enclave Protection	
Defense-in-Depth	Present
Firewalls	Present
Routers	Present
Switches	Present
Intrusion Detection System (IDS)	Present
Intrusion Prevention System (IPS)	Present
Demilitarized Zone (DMZ)	Present
Network Test Access Ports (TAP)	Absent
Wireless Intrusion Detection System (WIDS)	Absent
VPN Tunnel	Present
Firewalls	
Packet Filtering Firewall	Present
Bastion Host	Absent
Stateful Inspection Firewall	Present
Deep Packet Inspection Firewall	Absent
Application Proxy Gateway	Present
Proxy Server	Absent
Hybrid Technology Firewall	Absent
Routers	
Route Table Integrity	Present
Securing Router Planes	Absent

C] Network Infrastructure Security Risk Management Implementation controls and policies

Cybersecurity Implementation Controls	Implementation Status
Ports, Protocols, & Services	
Classification of Ports	Present
Restricting ICMPv4 Echo Request & Reply	Present
Preventing Traceroute	Present
IPv4 Address Filtering	Present
IPv6 Address Filtering	Absent
Unicast Reverse Path Forwarding	Absent
Protecting Servers from SYN Flood Attacks	Present
Device Management	
Vulnerability Management System	Absent
Software Updates	Present
Out-of-Band Management	Absent

In-Band Management	Present
Device Monitoring	
Simple Network Management Protocol	Present
Network Management Station	Present
Network Authentication, Authorization, & Accounting	
Authentication	Present
Authorization	Present
Accounting	Present
Auditing	Present
Router Password Protecting	Present
Network Intrusion Detection Systems (NIDS)	
Local Area NIDS	Present
External NIDS	Present
Switches & VLANs	
Physical Security	Present
VLANs	Present
VLAN Trunking	Absent
Port Security	Absent
801/1X & Management Policy Server	Present
Virtual Private Network	
Gateway to Gateway	Present
Host to Gateway	Present
Host to Host	Absent

D) Database Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls	Implementation Status
Authentication	
User Account	Present
Database Administrator (DBA)	Present
Application Owner	Present
Application User Manager	Present
Application Account	Present
Database Auditor	Present
Database Operator	Present
Passwords	Present
Certificates	Present
External Authentication	Present
Credentials Storage	Present
Authorization	
Role Based Access Control (RBAC)	Present

Renaming Default Accounts	Absent
Confidentiality	
Data Encryption	Present
Application Code Encryption	Present
Sensitive Data Encryption	Present
Data Integrity	
Data Integrity	Present
Transaction Logs	Present
Auditing	
Audit Logs	Present
Audit Logs Protection	Present
Audit Logs Storage	Present
Replication and Federation	
Database Replication	Present
Federated Database	Present
Database Clustering	
Database Clustering	Present
Principle of Least Privilege	Present
Accountability	Present
Backup and Recovery	
Testing and Maintenance	Present
Backup Encryption	Present
Backup Authentication & Authorization	Present
Operating Systems Protection	
Disk Partitions	Present
Separation of Accounts	Present
Database Software	Present
Application Protection	
Principle of least Privilege	Present
Auditing Elevated Privileges	Present
Input Validation	Present
Application Authentication	Present
Network Protections	
Network Access	Present
Limiting Network Session Parameters	Absent

Encryption	Present
Security Design & Configuration	
Procedural Review	Present
Configuration Specifications	Present
Compliance Testing	Present
Non- Repudiation	Present
Partitioning of the application	Present
Ports, Protocols, and services	Absent
Configuration Management Process	Absent
IA Documentation	Present
System library management controls	Present
Security Structure support partitioning	Present
System State Changes	Present
Software Baseline	Present
Group Identification and authentication	Present
Individual Identification and authentication	Present
Key Management	Absent
Token and certificate standards	Present
Enclave and Computing Environment	
Access for need to know	Absent
Audit Record content	Present
Audit trail, monitoring, analysis, and reporting	Present
Changes to data	Present
Encryption for Confidentiality	Present
Data change controls	Present
Interconnections among systems and enclaves	Present
Audit of security label changes	Present
Logon	Present
Least Privilege	Present
Marking and labeling	Present
Production code change controls	Present
Resource Control	Present
Audit reduction and report generation	Present
Audit Record Retention	Present
Security Configuration Compliance	Present

Software development change controls	Absent
Warning Messages	Present
Boundary defense	Absent
Business Continuity	
Protection of backup & Restoration Assets	Present
Data Backup Procedure	Present
Disaster & Recovery Plan	Absent
Backup of Critical Software	Present
Trusted Recovery	Present
Vulnerability & Incident Management	
Vulnerability Management	Present

E] Application Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls	Implementation Status
Application Data Handling	
Database Management System	Present
Data Storage	Present
In-Memory Data Handling	Present
Data Transmission	Present
Data Integrity	Present
Data Marking	Absent
Authentication	
Server Authentication	Present
User Authentication	Present
Signed Code Identification	Absent
Standalone Application Authentication	Present
Server Application Authentication	Present
Client Application Authentication	Absent
Combination Client Server Application Authentication	Present
Application Component Authentication	Present
Cryptography	
Symmetric Ciphers	Present
Message Authentication Code	Present
Digital Signature	Absent
User Accounts	
User Accounts	Present
Duplicate User Accounts	Present
Account Lockout Policy	Present
Application Sessions	Absent
Access Controls	Present
Input Validation	
Input Validation	Present
Input Sanitization	Absent

Static Analysis Tools	Present
Prepared Statements	Absent
Remove Hidden Fields	Present
Application Auditing	
Audit Scope	Present
Protecting Audit Trails	Present
Configuration Management	
Software Configuration Management	Present
Limiting Unauthorized Modification	Present
Testing	
Test Plans & Procedures	Present
Fuzzy Testing	Present
Code Reviews	Present
Automated Tools	Absent
Deployment	
Documentation	Present
Auditing	Present

F] Wireless Security Risk Management Implementation controls and Policies

Cybersecurity Implementation Controls	Implementation Status
Wireless LAN Risk Management	
IEEE 802.1x Extensible Authentication Protocol	Present
EAP Transport Layer Security (EAP-TLS)	Present
EAP Tunneling Transport Layer Security	Present
Protected Extensible Authentication Protocol (PEAP)	Absent
WLAN Components	Present
Access Point	Present
Separation of Networks	Present
Wi-fi Protected Access 2 (WPA2)	Present
VPN	Present
Access Point & Client Identification	Present
Security Boundary Implementations for DOD	Absent
Data-in-transit Encryption	Present
Wireless PAN Risk Management	
Bluetooth	Present
Pairing/Bonding	Present
Confidentiality	Present
Integrity	Present
Authentication	Present
Authorization	Present
Wireless PAN Risk Management	
Cellular Digital Packet Data	Present
Wireless RFID Risk Management	
Radio Frequency Identification	Present
Wireless PED Risk Management	
Subscriber Identity Module	Present
Wireless Two-Way Email	Present
PED Security	Absent

List of Potential Vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing.

- Unauthorized access
- Weak Authentication
- Broken Access Control
- Unauthorized modification
- Insecure code vulnerabilities
- Information disclosures
- Loss of integrity
- System Failure
- SQL injection
- Information Theft
- Man-in-the-Middle
- Data Tampering
- Data theft
- Interruption of Operations
- MAC Address Spoofing
- Network Misconfigurations
- Malware and Injection Attacks
- Denial Of Service (DoS)
- Network Infrastructure Attack
- Unpatched/obsolete software
- Compliance Violations
- Wireless Attack
- Firewall misconfiguration
- Weak Firewall Protection
- Privilege Escalation
- Network Session Hijacking
- Disruption of Business.

List of Potential Threats for critical assets where Cybersecurity Implementation Controls are missing.

- Loss of Confidentiality, Integrity, and Availability
- Loss of Data Privacy
- Information theft
- Interruption of Operations
- Unauthorized Access
- Non-Compliance Issues
- Data theft
- Data tampering
- Unauthorized use or disclosure of sensitive information
- Data corruption
- System instability
- Malware injection
- Loss of sensitive data

- Unauthorized data modification
- System downtime
- Inability to access critical systems
- Information Disclosure
- Loss of confidential data
- Identity theft
- Financial loss.

List of Potential Risks for critical assets where Cybersecurity Implementation Controls are missing.

- Security Breach
- Interruption of Operations
- Man-in-the-middle Attacks
- Denial Of Service Attacks
- Data Privacy Loss
- Non-Compliance Issues and fines
- Unavailability of business-critical assets and services
- Failure to achieve business objective
- Malware Attacks on OS
- Loss of integrity
- Insecure code vulnerabilities
- Unauthorized code modification
- Unauthorized access
- SQL injection
- System failure
- Data breach

List of recommended Hardening Prevention controls and policies for each recommended Control that should be created to reduce vulnerability probabilities and mitigate the identified risks

- Regular risk assessments must be conducted to identify risks, vulnerabilities and threats that are appropriate to the organization's business needs.
- Data in transit and static data must remain encrypted using robust encryption techniques that are secure and not obscure.
- Strong authentication techniques must be implied in the organization, like 2FA and MFA, to enhance role-based access control and increase accountability.
- Zero trust architecture and least privilege policy must be implemented in the network and systems.
- Segregation of systems and data must be conducted to keep data and systems safe in case of a security breach and reduce the scalabilities of a security breach.
- Intrusion Detection Systems (IDS) and Intrusion Prevention Systems (IPS) must be included in the architecture of the organization to enhance security.
- Firewall rules must be regularly reviewed and updated with changing business needs to increase efficiency and reduce false positives.
- Addition of Wireless Intrusion Detection System as well as Network Test Access Ports will increase wireless security.

- Insider threat and information theft policies must be created and maintained by enforcing stronger compliance and safety measures for all employees.
- Logical and physical boundaries must be created and planned better to increase the efficiency of the architecture and provide better defense.
- Security audits and compliance audits must be conducted regularly to assess the security status of the organization.
- Regular network scanning must be advised so as to identify the open ports and the services running so that better hardening controls can be implemented depending on the ports and services.
- There should be use of secure protocols and strong authentication mechanisms, restricting access to authorized personnel only, and monitoring and logging all activities for potential security threats.
- VLAN tagging should be implemented and encryption should be used to protect against VLAN hopping attacks, and regularly auditing and updating VLAN configurations to ensure they align with security policies.
- Use of strong encryption, mutual authentication, and access controls such as firewall rules and network segmentation should be implemented to prevent unauthorized access and protect the confidentiality and integrity of data transmitted over the VPN.

List of recommended Hardening Response controls and policies for each recommended control that should be created to reduce vulnerability probabilities and mitigate the identified risks.

- The Team must maintain and abide by the incident response plan and communicate with the incident response team as soon as an incident is detected.
- Logging and documentation of Incident response procedures must be performed to understand the lessons learned to update the incident response playbook in the future.
- A business continuity plan must be created to avoid irrational decisions in crucial moments of crisis and to keep the organization's flow moving with little to no disruption.
- All critical data and assets must be backed up in the organization and ready to download in an event of data loss or corruption.
- Updating to the latest version of all software in use around the organization is required, and also they must be licensed from a trusted source.
- Audit reports and monitor logs must be available for assessment in case of a security compromise.
- Updating and checking the operability of Intrusion prevention systems, Intrusion detection systems and antivirus in order to respond to a security threat at its earliest.
- All security incidents must be properly logged and reported to be used to improve the incident response playbook for future incidents.
- A business continuity plan and disaster recovery plan must be documented at the earliest and must be updated at least twice a year.
- Planning and establishing response controls to reduce the scale of an incident by assessing the organization's current security status that can be used in case of a security breach.
- Apply rules to restrict traffic to and from specified IPv6 addresses and to monitor and audit network traffic to ensure compliance with these rules.
- Enable strict mode and configure allowed and denied sources to prevent IP spoofing and ensure that traffic only comes from valid sources.

- Regular vulnerability scans should be conducted to prioritize and remediate high-risk vulnerabilities, and establish a patch management process to ensure that vulnerabilities are addressed promptly and efficiently.
- The team should use more secure protocols and strong authentication mechanisms, configure access controls to restrict access to authorized personnel, and log and monitor all activities on the out-of-band management network to detect and prevent security threats.
- Investigate to determine the cause and extent of the security incident, and take appropriate actions to remediate the issue.

Applicable Government Regulations and Industry Standards

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is an industry standard regulation in EU law that was created to strengthen data protection and privacy safeguards across the European Union (EU). The General Data Protection Regulation (GDPR) is an essential element of EU privacy law and human rights legislation, particularly Article 8 of the Charter of Fundamental Rights of the European Union (EU Charter). According to the General Data Protection Regulation (GDPR), a piece of information is considered "personal data" if it allows an individual to be directly or indirectly identified through the use of online identifiers such as their name, an identification number, an IP address, or their location data. Companies that do not comply or have a data breach may be subject to a financial penalty. In the most severe instances, this fine may be as high as 17 million euros, equivalent to four percent of a company's yearly revenue.

California Consumer Privacy Act of 2018 (CCPA)

The California Consumer Privacy Act of 2018 (CCPA) provides customers with increased control over the personal information collected about them by businesses, and the rules accompanying the legislation offer direction for how it should be implemented. Your personal information is any information that either identifies you or your household in some way, refers to you, or might fairly be associated with you. The customers must inform the firm of the specific CCPA regulations that were broken by the company and must allow the company thirty days to rectify the situation after receiving such notification. But, if the corporation does not rectify the issue, they risk being subject to statutory damages ranging from \$100 to \$750 for each harmed customer.

ISO 27001

Information security is governed by an international standard called ISO/IEC 27001. It outlines the requirements for an efficient ISMS (information security management system). The best-practice approach that ISO 27001 takes to managing information security helps organizations do so by focusing on three aspects: people, processes, and technology. Your information security management system's (ISMS) conformance to information security best practices may be validated globally by obtaining certification to the international standard ISO 27001

Rank Asset Risks and Vulnerability Risks for you company across Access Control, Network Infrastructure, Network Infrastructure Management, Database, Application and Wireless.

Domain	Top 5 Asset Risks	Top 5 Asset Vulnerabilities
Access Control	The absence of DOD Common Access Cards can lead to the loss of Integrity, privacy, and availability	Weak authentication
	No login tokens can lead to a loss of integrity, availability, and privacy	Unauthorized access
	In case of a social engineering attack, the identity of a user might be harder to determine without biometrics which can lead to a threat to sensitive data.	Information Theft
	Equipment failure can lead to discontinuity of functionalities.	Equipment failure
	Failed authorization can lead to compromising integrity and availability.	Social Engineering
Network Infrastructure	Lack of a bastion host increased the chances of penetration of a threat actor inside the network	Denial of Service Attacks
	Absence of Depp Packet Inspection Firewall can result in attacks on the application levels as malicious packets can be transferred without any detection.	Network infrastructure attack
	Absence of the proxy server can increase the possibility of an attack on active serves and in case the sever is compromised, all operations could be interrupted	Application layer attack
	Absence Hybrid Technology Firewall can result in attacks on the application levels as malicious packets can be transferred without any detection.	Network Port scan
	Absence of WIDS can increase the chances and scale of wireless attacks over the network	Wireless attack
Network Infrastructure Management	absence of IPv6 address filtering is the potential for unauthorized access or network-based attacks to occur via IPv6 traffic.	Malware and Injection Attacks
	absence of unicast reverse path forwarding is the possibility of malicious traffic entering the network and bypassing security mechanisms, leading to potential attacks or disruptions.	Denial of Service (DoS)
	not having a Vulnerability Management System is the increased likelihood of security vulnerabilities going undetected, leading to potential exploitation by attackers and compromise of critical assets.	Network Infrastructure Attack
	not having Out-of-band management is the potential for unauthorized access and control of network devices, leading to potential security breaches or disruptions.	Unpatched/obsolete Software
	not having port security is the potential for unauthorized devices to connect to a network and gain access to critical resources, leading to potential security breaches or disruptions.	Ip Address Spoofing
Database	Not controlling ports, protocols, and services increases the risk of unauthorized access, data theft, and other security breaches.	Broken Access Control

	Without a configuration management process, there is a risk of configuration drift and unauthorized changes to system configurations, which can lead to security vulnerabilities.	Unauthorized Access
	Without proper key management, there is a risk of data exposure, loss of confidentiality, and potential unauthorized access to sensitive information.	Disruption of Business
	Without software development change controls, there is a risk of introducing security vulnerabilities and errors into the software code.	Loss of Data
	Lack of boundary defense increases the risk of unauthorized access and data breaches, as well as external attacks on the system.	Privilege Escalation
Application	Absence or wrong marking of data can lead unauthorized users to be able to modify data.	Insecure code vulnerabilities
	If the source code is not signed, it allows unauthorized modifications and open doors to several insecure code vulnerabilities	Information disclosures
	Absence of this kind of authentication can lead to unauthorized access on the client side	Loss of integrity
	Can lead to a SQL injection attack and can open doors to other code related attacks	System failure
	Highly increases the risks of SQL injection due to the inability to use parametrized queries to handle the input given by the user.	SQL injection
Wireless	Absence can increase the risks of unauthorized access, which can lead to malicious attacks, information theft and data breaches	Unauthorized Access
	Absence can lead in the leaking of sensitive and classified information which can lead to vulnerabilities on the gateway	Information Disclosures
	Can lead to unauthorized access to sensitive data and a perfect loss of confidentiality and integrity	Broken Authentication
	Not having automated tools for testing can lead to a lot of insecure code vulnerabilities and system failure due to inability to use automate tools for code analysis and testing	Wireless Attacks
	host-to-host communication is the potential for unauthorized access or communication between hosts, leading to potential security breaches or data exfiltration.	Unauthorized Modifications

List of Top 5 Vulnerabilities:

- Unauthorized Modification
- Information Disclosure
- Denial of Service
- Disruption of Business-Critical Services
- Unauthorized Access

List of Top 5 Potential risks:

- Security Breach
- Data Privacy loss
- Failure to meet business goals
- Loss Of Confidentiality, Integrity and Availability
- Non- Compliance Issues and Heavy fines

List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerabilities and mitigate the identified risks- Risk Prevention Strategy

- Implement access control mechanisms to restrict access to sensitive data while also implementing encryption to protect data in transit and at rest
- Implement network segmentation to limit the impact of DoS attacks and implement rate limiting and traffic filtering to prevent DoS attacks
- Plan failover mechanisms to minimize the impact of service disruptions
- Implement disaster recovery and business continuity plans to minimize the impact of service disruptions
- Use multi-factor authentication (MFA)to prevent unauthorized access
- Use monitoring and auditing to detect and block unauthorized access attempts
- Implement privacy policies and procedures to ensure compliance with regulations (eg: GDPR)
- There should be monitoring and auditing to detect and block unauthorized access and modification
- Use security software to protect against malware and viruses
- Team should implement training and awareness programs to ensure employees understand and comply with cyber laws and regulations

List of recommended Hardening Response controls and policies for each recommended control that should be created to reduce vulnerabilities and mitigate the identified risks- Risk Response Strategy

- Implement strict access controls immediately to restrict modification of critical data and systems.
- Deploy security software that can detect and alert admins of any unauthorized modifications.
- Deploy monitoring software to detect and alert administrators of any unauthorized access to sensitive
- Develop, test and update incident response plans that can be quickly referred to in the event of a successful denial of service attack.
- DBMS backup must be ready for restoration almost immediately

- Implementing Intrusion Detection Systems all over the network can help monitor and detect suspicious activities.
- Implementing firewalls to block unauthorized access attempts and prevent network attacks
- Plan and document business continuity plan and disaster recovery plan.
- Maintain and update an incident response playbook for any events that might happen in the future.
- Plan and establish response controls to contain an incident by isolating the affected assets.
- Critical data loss prevention solutions must be implemented on the system and network to increase wireless security

Cybersecurity Workforce Risk Management Implementation

List of Cybersecurity Specialty areas that exist at Autumn-CSTL

Risk Management (RSK)
Software Development (DEV)
System Architecture (ARC)
Technology R&D (TRD)
Test and Evaluation (TST)
Systems Development (SYS)
Data Administration (DTA)
Customer Service and Technical Support (STS)
Systems Administration (ADM)
Systems Analysis (ANA)
Legal Advice and Advocacy (LGA)
Cybersecurity Management (MGT)
Strategic Planning and Policy (SPP)
Program/Project Management (PMA) and acquisition
Cybersecurity Defense Analysis (CDA)
Cybersecurity Defense Infrastructure Support (INF)
Incident Response (CIR)
Threat Analysis (TWA)
All-Source Analysis (ASA)
Collection Operations (CLO)
Cyber Operations (OPS)
Digital Forensics (FOR)

List of Cybersecurity roles that exist at Autumn-CSTL

Authorizing Official/Designating Representative
Security Control Assessor
Software Developer
Secure Software Assessor
Enterprise Architect
Security Architect
Research & Development Specialist
System Testing and Evaluation Specialist

Information Systems Security Developer
Systems Developer
Database Administrator
Data Analyst
Technical Support Specialist
System Administrator
Systems Security Analyst
Cyber Legal Advisor
Privacy Officer/Privacy Compliance Manager
Information Systems Security Manager
Cyber Workforce Developer and Manager
Program Manager
IT Program Auditor
Cyber Defense Analyst
Cyber Defense Infrastructure Support Specialist
Cyber Defense Incident Responder
Threat/Warning Analyst
All-Source Analyst
All Source-Collection Manager
Cyber Operator
Law Enforcement /Counter Intelligence Forensics Analyst
Cyber Defense Forensics Analyst

List of Cybersecurity Tasks that exist at Autumn-CSTL

Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.
Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
Assess the effectiveness of security controls.
Assess all the configuration management (change configuration/release management) processes.
Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.

Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.
Apply coding and testing standards, apply security testing tools including "fuzzing" static-analysis code scanning tools, and conduct code reviews.
Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.
Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.
Develop secure code and error handling.
Direct software programming and development of documentation.
Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.
Apply coding and testing standards, apply security testing tools including "fuzzing" static-analysis code scanning tools, and conduct code reviews.
Apply secure code documentation.
Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.
Develop threat model based on customer interviews and requirements.
Develop secure software testing and validation procedures.
Develop system testing and validation procedures, programming, and documentation.
Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
Employ secure configuration management processes.
Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.
Identify and prioritize critical business functions in collaboration with organizational stakeholders.
Provide advice on project costs, design concepts, or design changes.
Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
Analyze candidate architectures, allocate security services, and select security mechanisms.
Write detailed functional specifications that document the architecture development process.
Analyze user needs and requirements to plan architecture.
Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
Integrate results regarding the identification of gaps in security architecture.
Plan implementation strategy to ensure that enterprise components can be integrated and aligned.
Translate proposed capabilities into technical requirements.
Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture.
Integrate key management functions as related to cyberspace.
Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.

Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.
Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).
Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.
Provide advice on project costs, design concepts, or design changes.
Provide input on security requirements to be included in statements of work and other appropriate procurement documents.
Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
Write detailed functional specifications that document the architecture development process.
Analyze user needs and requirements to plan architecture.
Develop enterprise architecture or system components required to meet user needs.
Document and update as necessary all definition and architecture activities.
Review and validate data mining and data warehousing programs, processes, and requirements.
Research current technology to understand capabilities of required system or network.
Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.
Follow software and systems engineering life cycle standards and processes.
Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.
Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.
Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
Research and evaluate available technologies and standards to meet customer requirements.
Determine level of assurance of developed capabilities based on test results.
Develop test plans to address specifications and requirements.
Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.
Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
Create auditable evidence of security measures.
Validate specifications and requirements for testability.
Perform operational testing.
Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.
Record and manage test data.
Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
Develop detailed security design documentation for component and interface specifications to support system design and development.
Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.

Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.
Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
Provide support to security/certification test and evaluation activities.
Utilize models and simulations to analyze or predict system performance under different operating conditions.
Design to security requirements to ensure requirements are met for all systems and/or applications.
Develop mitigation strategies to address cost, schedule, performance, and security risks.
Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
Build, test, and modify product prototypes using working models or theoretical models.
Design and develop cybersecurity or cybersecurity-enabled products.
Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.
Develop and direct system testing and validation procedures and documentation.
Provide support to test and evaluation activities.
Trace system requirements to design components and perform gap analysis.
Verify stability, interoperability, portability, and/or scalability of system architecture.
Analyze user needs and requirements to plan and conduct system development.
Analyze and plan for anticipated changes in data capacity requirements.
Maintain database management systems software.
Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.
Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.
Maintain assured message delivery systems.
Implement data management standards, requirements, and specifications.
Implement data mining and data warehousing applications.
Analyze and define data requirements and specifications.
Analyze and plan for anticipated changes in data capacity requirements.
Develop data standards, policies, and procedures.
Manage the compilation, cataloging, caching, distribution, and retrieval of data.
Develop and facilitate data-gathering methods.
Develop strategic insights from large data sets.
Present technical information to technical and nontechnical audiences.
Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).
Develop and implement data mining and data warehousing programs.
Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
Troubleshoot system hardware and software.
Analyze incident data for emerging trends.
Develop and deliver technical training to educate others or meet customer needs.
Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.

Perform asset management/inventory of information technology (IT) resources.
Monitor and report client-level computer system performance.
Develop a trend analysis and impact report.
Conduct functional and connectivity testing to ensure continuing operability.
Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
Develop and document systems administration standard operating procedures.
Maintain baseline system security according to organizational policies.
Manage accounts, network rights, and access to systems and equipment.
Plan, execute, and verify data redundancy and system recovery procedures.
Install, update, and troubleshoot systems/servers.
Check system hardware availability, functionality, integrity, and efficiency.
Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.
Perform repairs on faulty system/server hardware.
Troubleshoot hardware/software interface and interoperability problems.
Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
Apply security policies to meet security objectives of the system.
Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.
Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.
Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.
Perform cybersecurity testing of developed applications and/or systems.
Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
Plan and recommend modifications or adjustments based on exercise results or system environment.
Assess and monitor cybersecurity related to system implementation and testing practices.
Verify minimum security requirements are in place for all applications.
Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.
Advocate organization's official position in legal and legislative proceedings.
Evaluate contracts to ensure compliance with funding, legal, and program requirements.
Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.
Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.
Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.
Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).
Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.
Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
Conduct functional and connectivity testing to ensure continuing operability.
Establish a risk management strategy for the organization that includes a determination of risk tolerance.

Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).
Develop and maintain strategic plans.
Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.
Liaise with regulatory and accrediting bodies.
Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.
Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security issues.
Work with organization senior management to establish an organization-wide Privacy Oversight Committee
Serve in a leadership role for Privacy Oversight Committee activities
Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices
Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations
Manage the monitoring of information security data sources to maintain organizational situational awareness.
Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.
Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.
Participate in an information security risk assessment during the Security Assessment and Authorization process.
Participate in the development or modification of the computer environment cybersecurity program plans and requirements.
Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.
Use federal and organization-specific published documents to manage operations of their computing environment system(s).
Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.
Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.
Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.
Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
Develop and implement standardized position descriptions based on established cyber work roles.
Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies.
Review and apply organizational policies related to or influencing the cyber workforce.
Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.

Support integration of qualified cyber workforce personnel into information systems life cycle development processes.
Develop and maintain strategic plans.
Develop methods to monitor and measure risk, compliance, and assurance efforts.
Perform needs analysis to determine opportunities for new and improved business process solutions.
Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).
Participate in the acquisition process as necessary.
Conduct import/export reviews for acquiring systems and software.
Develop methods to monitor and measure risk, compliance, and assurance efforts.
Provide ongoing optimization and problem-solving support.
Provide recommendations for possible improvements and upgrades.
Review or conduct audits of information technology (IT) programs and projects.
Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
Conduct import/export reviews for acquiring systems and software.
Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.
Develop content for cyber defense tools.
Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.
Coordinate with enterprise-wide cyber defense staff to validate network alerts.
Plan and recommend modifications or adjustments based on exercise results or system environment.
Provide daily summary reports of network events and activity relevant to cyber defense practices.
Examine network topologies to understand data flows through the network.
Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.
Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
Analyze and report system security posture trends.
Assess adequate access controls based on principles of least privilege and need-to-know.
Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.
Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.
Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.
Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).
Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.
Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).
Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.
Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.

Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.
Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.
Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
Track and document cyber defense incidents from initial detection through final resolution.
Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.
Coordinate with intelligence analysts to correlate threat assessment data.
Write and publish after action reviews.
Provide subject matter expertise to the development of cyber operations specific indicators.
Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
Assist in the identification of intelligence collection shortfalls.
Brief threat and/or target current situations.
Evaluate threat decision-making processes.
Identify threats to Blue Force vulnerabilities.
Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).
Report intelligence-derived significant network events and intrusions.
Generate requests for information.
Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
Assist in the identification of intelligence collection shortfalls.
Brief threat and/or target current situations.
Provide input and assist in post-action effectiveness assessments.
Provide input and assist in the development of plans and guidance.
Report intelligence-derived significant network events and intrusions.
Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.
Assess and apply operational environment factors and risks to collection management process.
Assess performance of collection assets against prescribed specifications.
Compare allocated and available assets to collection demand as expressed through requirements.
Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function.
Determine organizations and/or echelons with collection authority over all accessible collection assets.
Develop a method for comparing collection reports to outstanding requirements to identify information gaps.
Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources.
Specify discipline-specific collections and/or taskings that must be executed in the near term.
Conduct access enabling of wireless computer and digital networks.
Conduct collection and processing of wireless computer and digital networks.
Conduct exploitation of wireless computer and digital networks.
Facilitate access enabling by physical and/or wireless means.
Identify potential points of strength and vulnerability within a network.
Maintain situational awareness and functionality of organic operational infrastructure.

Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.
Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).
Resolve conflicts in laws, regulations, policies, standards, or procedures.
Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).
Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.
Analyze organizational cyber policy.
Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.
Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.
Perform hash comparison against established database.
Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).
Perform timeline analysis.
Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).
Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.
Coordinate with intelligence analysts to correlate threat assessment data.
Process image with appropriate tools depending on analyst's goals.

Comparison of the NCWF recommended cybersecurity specialty areas with Autumn-CSTL's Existing Cybersecurity Specialty Areas

Speciality Area	Status
Risk Management (RSK)	Present
Software Development (DEV)	Present
Systems Architecture (ARC)	Present
Technology R&D (TRD)	Present
Systems Requirements Planning (SRP)	Absent
Test and Evaluation (TST)	Present
Systems Development (SYS)	Present
Data Administration (DTA)	Present
Knowledge Management (KMG)	Absent
Customer Service and Technical Support (STS)	Present
Network Services (NET)	Absent
Systems Administration (ADM)	Present
Systems Analysis (ANA)	Present
Legal Advice and Advocacy (LGA)	Present
Training, Education, and Awareness (TEA)	Absent

Cybersecurity Management (MGT)	Present
Strategic Planning and Policy (SPP)	Present
Executive Cyber Leadership (EXL)	Absent
Program/Project Management (PMA) and Acquisition	Present
Cybersecurity Defense Analysis (CDA)	Present
Cybersecurity Defense Infrastructure Support (INF)	Present
Incident Response (CIR)	Present
Vulnerability Assessment and Management (VAM)	Absent
Threat Analysis (TWA)	Present
Exploitation Analysis (EXP)	Absent
All-Source Analysis (ASA)	Present
Targets (TGT)	Absent
Language Analysis (LNG)	Absent
Collection Operations (CLO)	Present
Cyber Operational Planning (OPL)	Absent
Cyber Operations (OPS)	Present
Cyber Investigation (INV)	Absent
Digital Forensics (FOR)	Present

Comparison of the NCWF recommended Cybersecurity Work roles with Autumn-CSTL's existing cybersecurity work roles and comparison of the NCWF recommended cybersecurity tasks with autumn-CSTL's existing Cybersecurity Tasks

Work Role	Tasks	Status
Authorizing Official/Designating Representative	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Present
	Establish acceptable limits for the software application, network, or system.	Present
	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
Security Control Assessor	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Present
	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Present
	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Absent
	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	Absent
	Establish acceptable limits for the software application, network, or system.	Absent
	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Absent
	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Present

	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Verify and update security documentation reflecting the application/system security design features.	Absent
	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Absent
	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Absent
	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Absent
	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Absent
	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Absent
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Present
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Present
	Assess the effectiveness of security controls.	Present
	Assess all the configuration management (change configuration/release management) processes.	Present
Software Developer	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	Present
	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	Present
	Apply coding and testing standards, apply security testing tools including "fuzzing" static-analysis code scanning tools, and conduct code reviews.	Present
	Apply secure code documentation.	Absent
	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Absent
	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	Absent
	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	Absent
	Consult with engineering staff to evaluate interface between hardware and software.	Absent
	Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.	Present
	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	Present
	Develop secure code and error handling.	Present

Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Absent
Identify basic common coding flaws at a high level.	Absent
Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.	Absent
Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Absent
Perform integrated quality assurance testing for security functionality and resiliency attack.	Absent
Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.	Absent
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.	Absent
Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Absent
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Absent
Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Absent
Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.	Absent
Identify and leverage the enterprise-wide version control system while designing and developing secure applications.	Absent
Consult with customers about software system design and maintenance.	Absent
Direct software programming and development of documentation.	Present
Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Present
Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	Present
Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.	Absent
Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.	Absent
Develop software system testing and validation procedures, programming, and documentation.	Absent
Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.	Absent
Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Absent
Determine and document software patches or the extent of releases that would leave software vulnerable.	Absent

Secure Software Absent Assessor	Apply coding and testing standards, apply security testing tools including "fuzzing" static-analysis code scanning tools, and conduct code reviews.	Present
	Apply secure code documentation.	Present
	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Present
	Develop threat model based on customer interviews and requirements.	Present
	Consult with engineering staff to evaluate interface between hardware and software.	Absent
	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Absent
	Identify basic common coding flaws at a high level.	Absent
	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.	Absent
	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Absent
	Perform integrated quality assurance testing for security functionality and resiliency attack.	Absent
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Absent
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Absent
	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Absent
	Perform penetration testing as required for new or updated applications.	Absent
	Consult with customers about software system design and maintenance.	Absent
	Direct software programming and development of documentation.	Absent
	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Absent
	Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.	Absent
	Absent Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.	Absent
	Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.	Absent
	Develop secure software testing and validation procedures.	Present
	Develop system testing and validation procedures, programming, and documentation.	Present
	Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.	Absent
	Determine and document software patches or the extent of releases that would leave software vulnerable.	Absent

Enterprise Architect	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Present
	Employ secure configuration management processes.	Present
	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Present
	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Present
	Provide advice on project costs, design concepts, or design changes.	Present
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Present
	Analyze candidate architectures, allocate security services, and select security mechanisms.	Present
	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Absent
	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Absent
	Write detailed functional specifications that document the architecture development process.	Present
	Analyze user needs and requirements to plan architecture.	Present
	Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Present
	Develop enterprise architecture or system components required to meet user needs.	Absent
	Document and update as necessary all definition and architecture activities.	Absent
	Integrate results regarding the identification of gaps in security architecture.	Present
	Plan implementation strategy to ensure that enterprise components can be integrated and aligned.	Present
	Translate proposed capabilities into technical requirements.	Present
	Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture.	Present
	Integrate key management functions as related to cyberspace.	Present
Security Architect	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Present
	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Present
	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).	Present

	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.	Present
	Employ secure configuration management processes.	Absent
	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Absent
	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Absent
	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Absent
	Provide advice on project costs, design concepts, or design changes.	Present
	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	Present
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Present
	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Absent
	Analyze candidate architectures, allocate security services, and select security mechanisms.	Absent
	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Absent
	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Absent
	Write detailed functional specifications that document the architecture development process.	Present
	Analyze user needs and requirements to plan architecture.	Present
	Develop enterprise architecture or system components required to meet user needs.	Present
	Document and update as necessary all definition and architecture activities.	Present
	Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.	Absent
	Translate proposed capabilities into technical requirements.	Absent
	Assess and design security management functions as related to cyberspace.	Absent
Research & Development Specialist	Review and validate data mining and data warehousing programs, processes, and requirements.	Present
	Research current technology to understand capabilities of required system or network.	Present
	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.	Present
	Collaborate with stakeholders to identify and/or develop appropriate solutions technology.	Absent
	Design and develop new tools/technologies as related to cybersecurity.	Absent
	Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.	Absent
	Follow software and systems engineering life cycle standards and processes.	Present
	Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.	Present

	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.	Present
	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Present
	Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce.	Absent
	Research and evaluate available technologies and standards to meet customer requirements.	Present
Systems Requirements Planner	Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.	Absent
	Consult with customers to evaluate functional requirements.	Absent
	Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.	Absent
	Define project scope and objectives based on customer requirements.	Absent
	Develop and document requirements, capabilities, and constraints for design procedures and processes.	Absent
	Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.	Absent
	Oversee and make recommendations regarding configuration management.	Absent
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Absent
	Prepare use cases to justify the need for specific information technology (IT) solutions.	Absent
	Translate functional requirements into technical solutions.	Absent
	Develop and document supply chain risks for critical system elements, as appropriate.	Absent
	Develop and document User Experience (UX) requirements including information architecture and user interface requirements.	Absent
	Design and document quality standards.	Absent
	Document a system's purpose and preliminary system security concept of operations.	Absent
	Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).	Absent
	Define baseline security requirements in accordance with applicable guidelines.	Absent
	Develop cost estimates for new or modified system(s).	Absent
	Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.	Absent
System Testing and Evaluation Specialist	Determine level of assurance of developed capabilities based on test results.	Present
	Develop test plans to address specifications and requirements.	Present
	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Absent
	Make recommendations based on test results.	Absent
	Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.	Present
	Create auditable evidence of security measures.	Present
	Validate specifications and requirements for testability.	Present
	Analyze the results of software, hardware, or interoperability testing.	Absent
	Perform developmental testing on systems under development.	Absent

	Perform interoperability testing on systems exchanging electronic information with other systems.	Absent
	Perform operational testing.	Present
	Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.	Present
	Record and manage test data.	Present
Information Systems Security Developer	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Present
	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Present
	Assess the effectiveness of cybersecurity measures utilized by system(s).	Absent
	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	Absent
	Build, test, and modify product prototypes using working models or theoretical models.	Absent
	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Absent
	Design and develop cybersecurity or cybersecurity-enabled products.	Absent
	Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.	Absent
	Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Absent
	Develop and direct system testing and validation procedures and documentation.	Absent
	Develop detailed security design documentation for component and interface specifications to support system design and development.	Present
	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Present
	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.	Present
	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.	Absent
	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.	Absent
	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Absent
	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Absent
	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.	Absent
	Implement security designs for new or existing system(s).	Absent
	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).	Absent

	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
	Provide guidelines for implementing developed systems to customers or installation teams.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Present
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Present
	Provide support to security/certification test and evaluation activities.	Present
	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Present
	Design and develop key management functions (as related to cybersecurity).	Absent
	Analyze user needs and requirements to plan and conduct system security development.	Absent
	Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	Absent
	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Absent
	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Absent
	Employ configuration management processes.	Absent
	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Absent
	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	Absent
	Design to security requirements to ensure requirements are met for all systems and/or applications.	Present
	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Present
	Perform an information security risk assessment.	Absent
	Perform security reviews and identify security gaps in architecture.	Absent
	Provide input to implementation plans and standard operating procedures as they relate to information systems security.	Absent
	Trace system requirements to design components and perform gap analysis.	Absent
	Verify stability, interoperability, portability, and/or scalability of system architecture.	Absent
Systems Developer	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Present
	Build, test, and modify product prototypes using working models or theoretical models.	Present
	Design and develop cybersecurity or cybersecurity-enabled products.	Present
	Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Present
	Develop and direct system testing and validation procedures and documentation.	Present

	Develop architectures or system components consistent with technical specifications.	Absent
	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Absent
	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Absent
	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Absent
	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.	Absent
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
	Provide guidelines for implementing developed systems to customers or installation teams.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Absent
	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Absent
	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Absent
	Employ configuration management processes.	Absent
	Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	Absent
	Design and develop system administration and management functionality for privileged access users.	Absent
	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Absent
	Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle).	Absent
	Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.	Absent
	Design hardware, operating systems, and software applications to adequately address requirements.	Absent
	Design to security requirements to ensure requirements are met for all systems and/or applications.	Absent
	Develop detailed design documentation for component and interface specifications to support system design and development.	Absent
	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Absent

	Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.	Absent
	Implement designs for new or existing system(s).	Absent
	Perform security reviews and identify security gaps in architecture.	Absent
	Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials	Absent
	Provide support to test and evaluation activities.	Present
	Trace system requirements to design components and perform gap analysis.	Present
	Verify stability, interoperability, portability, and/or scalability of system architecture.	Present
	Analyze user needs and requirements to plan and conduct system development.	Present
	Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.	Absent
	Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	Absent
Database Administrator	Analyze and plan for anticipated changes in data capacity requirements.	Present
	Maintain database management systems software.	Present
	Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.	Present
	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.	Present
	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Absent
	Monitor and maintain databases to ensure optimal performance.	Absent
	Perform backup and recovery of databases to ensure data integrity.	Absent
	Provide recommendations on new database technologies and architectures.	Absent
	Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.	Absent
	Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.	Absent
	Maintain assured message delivery systems.	Present
	Implement data management standards, requirements, and specifications.	Present
	Implement data mining and data warehousing applications.	Present
	Install and configure database management systems and software.	Absent
Data Analyst	Analyze and define data requirements and specifications.	Present
	Analyze and plan for anticipated changes in data capacity requirements.	Present
	Develop data standards, policies, and procedures.	Present
	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Present
	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.	Absent
	Provide recommendations on new database technologies and architectures.	Absent
	Analyze data sources to provide actionable recommendations.	Absent
	Assess the validity of source data and subsequent findings.	Absent
	Collect metrics and trending data.	Absent
	Conduct hypothesis testing using statistical processes.	Absent

	Confer with systems analysts, engineers, programmers, and others to design application.	Absent
	Develop and facilitate data-gathering methods.	Present
	Develop strategic insights from large data sets.	Present
	Present technical information to technical and nontechnical audiences.	Present
	Present data in creative formats.	Absent
	Program custom algorithms.	Absent
	Provide actionable recommendations to critical stakeholders based on data analysis and findings.	Absent
	Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.	Absent
	Effectively allocate storage capacity in the design of data management systems.	Absent
		Absent
	Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	Absent
	Utilize different programming languages to write code, open files, read files, and write output to different files.	Absent
	Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).	Present
	Develop and implement data mining and data warehousing programs.	Present
Knowledge Manager	Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.	Absent
	Develop an understanding of the needs and requirements of information end-users.	Absent
	Monitor and report the usage of knowledge management assets and resources.	Absent
	Plan and manage the delivery of knowledge management projects.	Absent
	Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information.	Absent
	Lead efforts to promote the organization's use of knowledge management and information sharing.	Absent
	Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).	Absent
	Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization's intellectual capital.	Absent
	Promote knowledge sharing between information owners/users through an organization's operational processes and systems.	Absent
Technical Support Specialist	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Present
	Troubleshoot system hardware and software.	Present
	Analyze incident data for emerging trends.	Present
	Develop and deliver technical training to educate others or meet customer needs.	Present
	Maintain incident tracking and solution database.	Absent
	Diagnose and resolve customer reported system incidents, problems, and events.	Absent
	Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.	Present

	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	Absent
	Administer accounts, network rights, and access to systems and equipment.	Absent
	Perform asset management/inventory of information technology (IT) resources.	Present
	Monitor and report client-level computer system performance.	Present
	Develop a trend analysis and impact report.	Present
Network Operations Specialist	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).	Absent
	Develop and implement network backup and recovery procedures.	Absent
	Diagnose network connectivity problem.	Absent
	Implement new system design procedures, test procedures, and quality standards.	Absent
	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Absent
	Install or replace network hubs, routers, and switches.	Absent
	Integrate new systems into existing network architecture.	Absent
	Monitor network capacity and performance.	Absent
	Patch network vulnerabilities to ensure that information is safeguarded against outside parties.	Absent
	Provide feedback on network requirements, including network architecture and infrastructure.	Absent
System Administrator	Test and maintain network infrastructure including software and hardware devices.	Absent
	Conduct functional and connectivity testing to ensure continuing operability.	Present
	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	Present
	Develop and document systems administration standard operating procedures.	Present
	Maintain baseline system security according to organizational policies.	Present
	Manage accounts, network rights, and access to systems and equipment.	Present
	Plan, execute, and verify data redundancy and system recovery procedures.	Present
	Provide ongoing optimization and problem-solving support.	Absent
	Install, update, and troubleshoot systems/servers.	Present
	Check system hardware availability, functionality, integrity, and efficiency.	Present
	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	Present
	Comply with organization systems administration standard operating procedures.	Absent
	Implement and enforce local network usage policies and procedures.	Absent
	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	Absent
	Monitor and maintain system/server configuration.	Absent
	Oversee installation, implementation, configuration, and support of system components.	Absent
	Diagnose faulty system/server hardware.	Absent
	Perform repairs on faulty system/server hardware.	Present
	Troubleshoot hardware/software interface and interoperability problems.	Present
Systems Security Analyst	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Present
	Apply security policies to meet security objectives of the system.	Present
	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	Present

	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Absent
	Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.	Present
	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Present
	Implement specific cybersecurity countermeasures for systems and/or applications.	Absent
	Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.	Absent
	Perform cybersecurity testing of developed applications and/or systems.	Present
	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Present
	Plan and recommend modifications or adjustments based on exercise results or system environment.	Present
	Properly document all systems security implementation, operations, and maintenance activities and update as necessary.	Absent
	Provide cybersecurity guidance to leadership.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Verify and update security documentation reflecting the application/system security design features.	Absent
	Assess the effectiveness of security controls.	Absent
	Assess all the configuration management (change configuration/release management) processes.	Absent
	Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.	Absent
	Analyze and report organizational security posture trends.	Absent
	Analyze and report system security posture trends.	Absent
	Assess adequate access controls based on principles of least privilege and need-to-know.	Absent
	Ensure the execution of disaster recovery and continuity of operations.	Absent
	Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed.	Absent
	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Absent
	Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment.	Absent
	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.	Absent
	Assess and monitor cybersecurity related to system implementation and testing practices.	Present
	Verify minimum security requirements are in place for all applications.	Present

	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Present
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Absent
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Absent
Cyber Legal Advisor	Advocate organization's official position in legal and legislative proceedings.	Present
	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Present
	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.	Present
	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	Absent
	Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.	Absent
	Develop guidelines for implementation.	Absent
	Provide legal analysis and decisions to inspectors general, privacy officers, oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements.	Absent
	Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.	Present
	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Present
	Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.	Present
Privacy Officer/Privacy Compliance Manager	Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).	Present
	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Present
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Present
	Conduct functional and connectivity testing to ensure continuing operability.	Present
	Establish a risk management strategy for the organization that includes a determination of risk tolerance.	Present
	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Present
	Develop and maintain strategic plans.	Present
	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Absent
	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Absent
	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Absent
	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Absent

	Present technical information to technical and nontechnical audiences.	Absent
	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Absent
	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Absent
	Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.	Absent
	Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.	Absent
	Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.	Present
	Liaise with regulatory and accrediting bodies.	Present
	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.	Present
	Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.	Absent
	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.	Absent
	Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues.	Present
	Work with organization senior management to establish an organization-wide Privacy Oversight Committee	Present
	Serve in a leadership role for Privacy Oversight Committee activities	Present
	Collaborate on cyber privacy and security policies and procedures	Absent
	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation	Absent
	Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations	Absent
	Provide strategic guidance to corporate officers regarding information resources and technology	Absent
	Assist the Security Officer with the development and implementation of an information infrastructure	Absent
	Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations.	Present
	Work cooperatively with applicable organization units in overseeing consumer information access rights	Absent
	Serve as the information privacy liaison for users of technology systems	Absent
	Act as a liaison to the information systems department	Absent
	Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Absent
	Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties	Absent

	Conduct on-going privacy training and awareness activities	Absent
	Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security	Absent
	Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.	Absent
	Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee	Absent
	Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data	Absent
	Provide leadership for the organization's privacy program	Absent
	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization	Absent
	Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable	Absent
	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures	Absent
	Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices	Absent
	Develop and coordinate a risk management and compliance framework for privacy	Absent
	Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.	Absent
	Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations	Absent
	Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization's privacy policies and procedures	Absent
	Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity	Absent
	Provide leadership in the planning, design and evaluation of privacy and security related projects	Absent
	Establish an internal privacy audit program	Absent
	Periodically revise the privacy program considering changes in laws, regulatory or company policy	Absent
	Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel	Absent
	Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information	Absent

	Monitor systems development and operations for security and privacy compliance	Absent
	Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected	Absent
	Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions	Absent
	Review all system-related information security plans to ensure alignment between security and privacy practices	Absent
	Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements	Absent
	Account for and administer individual requests for release or disclosure of personal and/or protected information	Absent
	Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements	Absent
	Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed	Absent
	Act as, or work with, counsel relating to business partner contracts	Absent
	Mitigate effects of a use or disclosure of personal information by employees or business partners	Absent
	Develop and apply corrective action procedures	Absent
	Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel	Absent
	Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations	Absent
	Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations	Absent
	Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units	Absent
	Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices	Absent
	Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations	Present
	Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials	Absent
Cyber Instructional Curriculum Developer	Support the design and execution of exercise scenarios.	Absent
	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Absent
	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Absent
	Research current technology to understand capabilities of required system or network.	Absent
	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.	Absent
	Conduct learning needs assessments and identify requirements.	Absent

	Create interactive learning exercises to create an effective learning environment.	Absent
	Develop or assist in the development of training policies and protocols for cyber training.	Absent
	Develop the goals and objectives for cyber curriculum.	Absent
	Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.	Absent
	Correlate training and learning to business or mission requirements.	Absent
	Create training courses tailored to the audience and physical environment.	Absent
	Design training curriculum and course content based on requirements.	Absent
	Participate in development of training curriculum and course content.	Absent
	Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).	Absent
	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Absent
	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.	Absent
Cyber Instructor	Conduct interactive training exercises to create an effective learning environment.	Absent
	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	Absent
	Evaluate the effectiveness and comprehensiveness of existing training programs.	Absent
	Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).	Absent
	Support the design and execution of exercise scenarios.	Absent
	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Absent
	Develop or assist in the development of computer based training modules or classes.	Absent
	Develop or assist in the development of course assignments.	Absent
	Develop or assist in the development of course evaluations.	Absent
	Develop or assist in the development of grading and proficiency standards.	Absent
	Assist in the development of individual/collective development, training, and/or remediation plans.	Absent
	Develop or assist in the development of learning objectives and goals.	Absent
	Develop or assist in the development of on-the-job training materials or programs.	Absent
	Develop or assist in the development of written tests for measuring and assessing learner proficiency.	Absent
	Conduct learning needs assessments and identify requirements.	Absent
	Develop or assist in the development of training policies and protocols for cyber training.	Absent
	Develop the goals and objectives for cyber curriculum.	Absent
	Present technical information to technical and nontechnical audiences.	Absent
	Present data in creative formats.	Absent
	Write and publish after action reviews.	Absent

	Deliver training courses tailored to the audience and physical/virtual environments.	Absent
	Apply concepts, procedures, software, equipment, and/or technology applications to students.	Absent
	Design training curriculum and course content based on requirements.	Absent
	Participate in development of training curriculum and course content.	Absent
	Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.	Absent
	Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment.	Absent
	Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).	Absent
	Recommend revisions to curriculum and course content based on feedback from previous training sessions.	Absent
	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Absent
	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.	Absent
Information Systems Security Manager	Manage the monitoring of information security data sources to maintain organizational situational awareness.	Present
	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Present
	Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.	Present
	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	Absent
	Oversee the information security training and awareness program.	Absent
	Participate in an information security risk assessment during the Security Assessment and Authorization process.	Present
	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	Present
	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.	Absent
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Absent
	Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.	Absent
	Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	Absent
	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.	Absent
	Recognize a possible security violation and take appropriate action to report the incident, as required.	Absent
	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.	Absent

	Recommend policy and coordinate review and approval.	Absent
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Present
	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.	Present
	Use federal and organization-specific published documents to manage operations of their computing environment system(s).	Present
	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Absent
	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Absent
	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.	Absent
	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Absent
	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Absent
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Absent
	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.	Absent
	Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.	Present
	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Present
Communications Security (COMSEC) Manager	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Absent
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Absent
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Absent
	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Absent
	Ensure that security improvement actions are evaluated, validated, and implemented as required.	Absent
	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Absent
	Recognize a possible security violation and take appropriate action to report the incident, as required.	Absent

	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
Cyber Workforce Developer and Manager	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Present
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Present
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Present
	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Absent
	Develop policy, programs, and guidelines for implementation.	Absent
	Establish and maintain communication channels with stakeholders.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Absent
	Identify organizational policy stakeholders.	Absent
	Review existing and proposed policies with stakeholders.	Absent
	Serve on agency and interagency policy boards.	Absent
	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Absent
	Conduct learning needs assessments and identify requirements.	Absent
	Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.	Absent
	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Absent
	Develop and implement standardized position descriptions based on established cyber work roles.	Present
	Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies.	Present
	Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.	Absent
	Develop or assist in the development of training policies and protocols for cyber training.	Absent
	Ensure that cyber career fields are managed in accordance with organizational HR policies and directives.	Absent
	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	Absent
	Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.	Absent
	Establish and oversee waiver processes for cyber career field entry and training qualification requirements.	Absent
	Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.	Absent
	Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.	Absent
	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	Absent

	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Absent
	Review and apply cyber career field qualification standards.	Absent
	Review and apply organizational policies related to or influencing the cyber workforce.	Present
	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Present
	Support integration of qualified cyber workforce personnel into information systems life cycle development processes.	Present
	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Absent
	Analyze organizational cyber policy.	Absent
	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Absent
	Correlate training and learning to business or mission requirements.	Absent
	Define and integrate current and future mission environments.	Absent
	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Absent
	Draft, staff, and publish cyber policy.	Absent
	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Absent
	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Absent
	Seek consensus on proposed policy changes from stakeholders.	Absent
	Provide policy guidance to cyber management, staff, and users.	Absent
	Review, conduct, or participate in audits of cyber programs and projects.	Absent
	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Absent
	Support the CIO in the formulation of cyber-related policies.	Absent
	Review and approve a supply chain security/risk management policy.	Absent
Cyber Policy and Strategy Planner	Develop policy, programs, and guidelines for implementation.	Absent
	Establish and maintain communication channels with stakeholders.	Absent
	Review existing and proposed policies with stakeholders.	Absent
	Serve on agency and interagency policy boards.	Absent
	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Absent
	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	Absent
	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Absent
	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Absent
	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Absent
	Analyze organizational cyber policy.	Absent

	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Absent
	Define and integrate current and future mission environments.	Absent
	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Absent
	Draft, staff, and publish cyber policy.	Absent
	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Absent
	Seek consensus on proposed policy changes from stakeholders.	Absent
	Provide policy guidance to cyber management, staff, and users.	Absent
	Review, conduct, or participate in audits of cyber programs and projects.	Absent
	Support the CIO in the formulation of cyber-related policies.	Absent
Executive Cyber Leadership	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Absent
	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Absent
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Absent
	Advocate organization's official position in legal and legislative proceedings.	Absent
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Absent
	Develop and maintain strategic plans.	Absent
	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.	Absent
	Lead and align information technology (IT) security priorities with the security strategy.	Absent
	Lead and oversee information security budget, staffing, and contracting.	Absent
	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Absent
	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	Absent
	Recommend policy and coordinate review and approval.	Absent
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Absent
	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Absent
	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.	Absent
	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Absent
	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Absent

	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Absent
	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Absent
	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Absent
	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan.	Absent
	Perform an information security risk assessment.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
	Collaborate on cyber privacy and security policies and procedures	Absent
	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation	Absent
	Appoint and guide a team of IT security experts.	Absent
	Collaborate with key stakeholders to establish a cybersecurity risk management program.	Absent
Program Manager	Develop and maintain strategic plans.	Present
	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Present
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Present
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Develop and document supply chain risks for critical system elements, as appropriate.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Develop contract language to ensure supply chain, system, network, and operational security are met.	Absent
	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Absent
	Coordinate and manage the overall service provided to a customer end-to-end.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Present
	Participate in the acquisition process as necessary.	Present
	Conduct import/export reviews for acquiring systems and software.	Present
	Develop supply chain, system, network, performance, and cybersecurity requirements.	Absent
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent

	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Absent
	Lead and oversee budget, staffing, and contracting.	Absent
	Draft and publish supply chain security and risk management documents.	Absent
IT Project Manager	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Absent
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Absent
	Provide advice on project costs, design concepts, or design changes.	Absent
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Absent
	Provide ongoing optimization and problem-solving support.	Absent
	Provide recommendations for possible improvements and upgrades.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Develop and document supply chain risks for critical system elements, as appropriate.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Absent
	Coordinate and manage the overall service provided to a customer end-to-end.	Absent
	Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Absent
	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Absent
	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Absent
	Participate in the acquisition process as necessary.	Absent
	Conduct import/export reviews for acquiring systems and software.	Absent
	Develop supply chain, system, network, performance, and cybersecurity requirements.	Absent
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent
	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Absent
	Lead and oversee budget, staffing, and contracting.	Absent
	Draft and publish supply chain security and risk management documents.	Absent
	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Absent

Product Support Manager	Perform needs analysis to determine opportunities for new and improved business process solutions.	Absent
	Provide advice on project costs, design concepts, or design changes.	Absent
	Provide input to implementation plans and standard operating procedures.	Absent
	Provide ongoing optimization and problem-solving support.	Absent
	Provide recommendations for possible improvements and upgrades.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Develop and document supply chain risks for critical system elements, as appropriate.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Develop contract language to ensure supply chain, system, network, and operational security are met.	Absent
	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Absent
	Coordinate and manage the overall service provided to a customer end-to-end.	Absent
	Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Absent
	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Absent
	Conduct import/export reviews for acquiring systems and software.	Absent
	Develop supply chain, system, network, performance, and cybersecurity requirements.	Absent
	Lead and oversee budget, staffing, and contracting.	Absent
IT Investment/Portfolio Manager	Provide enterprise cybersecurity and supply chain risk management guidance.	Absent
	Draft and publish supply chain security and risk management documents.	Absent
	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Develop contract language to ensure supply chain, system, network, and operational security are met.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent
	Lead and oversee budget, staffing, and contracting.	Absent

	Draft and publish supply chain security and risk management documents.	Absent
IT Program Auditor	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Absent
	Provide ongoing optimization and problem-solving support.	Present
	Provide recommendations for possible improvements and upgrades.	Present
	Review or conduct audits of information technology (IT) programs and projects.	Present
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Present
	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Absent
	Conduct import/export reviews for acquiring systems and software.	Present
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Present
Cyber Defense Analyst	Develop content for cyber defense tools.	Present
	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Present
	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Present
	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Absent
	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	Absent
	Perform cyber defense trend analysis and reporting.	Absent
	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.	Absent
	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Absent
	Plan and recommend modifications or adjustments based on exercise results or system environment.	Absent
	Provide daily summary reports of network events and activity relevant to cyber defense practices.	Absent
	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Present
	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.	Absent
	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Absent
	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	Absent
	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.	Absent
	Examine network topologies to understand data flows through the network.	Present
	Recommend computing environment vulnerability corrections.	Absent
	Identify and analyze anomalies in network traffic using metadata.	Absent
	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).	Absent
	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	Present

	Isolate and remove malware.	Absent
	Identify applications and operating systems of a network device based on network traffic.	Absent
	Reconstruct a malicious attack or activity based off network traffic.	Absent
	Identify network mapping and operating system (OS) fingerprinting activities.	Absent
	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.	Absent
	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.	Absent
	Analyze and report organizational security posture trends.	Absent
	Analyze and report system security posture trends.	Present
	Assess adequate access controls based on principles of least privilege and need-to-know.	Present
	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.	Absent
	Assess and monitor cybersecurity related to system implementation and testing practices.	Absent
	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Absent
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Absent
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Absent
Cyber Defense Infrastructure Support Specialist	Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.	Present
	Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.	Present
	Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.	Present
	Build, install, configure, and test dedicated cyber defense hardware.	
	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.	Present
	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).	
	Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).	Present
	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).	Present
	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.	Present

Cyber Defense Incident Responder	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.	Present
	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.	Present
	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.	Present
	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.	Absent
	Perform cyber defense trend analysis and reporting.	Absent
	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.	Absent
	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	Absent
	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Present
	Track and document cyber defense incidents from initial detection through final resolution.	Present
	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.	Present
	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).	Absent
	Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Absent
	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Absent
	Coordinate with intelligence analysts to correlate threat assessment data.	Present
	Write and publish after action reviews.	Present
	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.	Absent
	Coordinate incident response functions.	Absent
Vulnerability Assessment Analyst	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	Absent
	Conduct and/or support authorized penetration testing on enterprise network assets.	Absent
	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.	Absent
	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	Absent
	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Absent
	Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).	Absent

	Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).	Absent
	Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).	Absent
Threat/Warning Analyst	Answer requests for information.	Absent
	Provide subject matter expertise to the development of a common operational picture.	Present
	Maintain a common intelligence picture.	Absent
	Provide subject matter expertise to the development of cyber operations specific indicators.	Absent
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Present
	Assist in the identification of intelligence collection shortfalls.	Present
	Brief threat and/or target current situations.	Present
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Conduct in-depth research and analysis.	Absent
	Conduct nodal analysis.	Absent
	Develop information requirements necessary for answering priority information requests.	Absent
	Evaluate threat decision-making processes.	Present
	Identify threats to Blue Force vulnerabilities.	Present
	Generate requests for information.	Present
	Identify threat tactics, and methodologies.	Absent
	Identify intelligence gaps and shortfalls.	Absent
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Absent
	Monitor and report on validated threat activities.	Absent
	Monitor open source websites for hostile content directed towards organizational or partner interests.	Absent
	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Absent
	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Present
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Absent
	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Absent
	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Absent
	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Absent
	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	Absent

	Report intelligence-derived significant network events and intrusions.	Present
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Absent
Exploitation Analyst	Conduct and/or support authorized penetration testing on enterprise network assets.	Absent
	Perform penetration testing as required for new or updated applications.	Absent
	Apply and utilize authorized cyber capabilities to enable access to targeted networks.	Absent
	Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements.	Absent
	Apply and obey applicable statutes, laws, regulations and policies.	Absent
	Perform analysis for target infrastructure exploitation activities.	Absent
	Collaborate with other internal and external partner organizations on target access and operational issues.	Absent
	Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.	Absent
	Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.	Absent
	Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.	Absent
	Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities.	Absent
	Examine intercept-related metadata and content with an understanding of targeting significance.	Absent
	Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.	Absent
	Identify gaps in our understanding of target technology and developing innovative collection approaches.	Absent
	Identify, locate, and track targets via geospatial analysis techniques.	Absent
	Lead or enable exploitation operations in support of organization objectives and target requirements.	Absent
	Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.	Absent
	Monitor target networks to provide indications and warning of target communications changes or processing failures.	Absent
	Produce network reconstructions.	Absent
	Profile network or system administrators and their activities.	Absent
All-Source Analyst	Answer requests for information.	Absent
	Provide expertise to course of action development.	Absent
	Provide subject matter expertise to the development of a common operational picture.	Absent
	Maintain a common intelligence picture.	Absent
	Provide subject matter expertise to the development of cyber operations specific indicators.	Absent
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Present
	Assist in the identification of intelligence collection shortfalls.	Present
	Brief threat and/or target current situations.	Present

	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Conduct in-depth research and analysis.	Absent
	Conduct nodal analysis.	Absent
	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	Absent
	Develop information requirements necessary for answering priority information requests.	Absent
	Engage customers to understand customers' intelligence needs and wants.	Absent
	Evaluate threat decision-making processes.	Absent
	Identify threat vulnerabilities.	Absent
	Identify threats to Blue Force vulnerabilities.	Absent
	Generate requests for information.	Absent
	Identify threat tactics, and methodologies.	Absent
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Absent
	Identify and submit intelligence requirements for the purposes of designating priority information requirements.	Absent
	Identify intelligence gaps and shortfalls.	Absent
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Absent
	Monitor and report on validated threat activities.	Absent
	Monitor open source websites for hostile content directed towards organizational or partner interests.	Absent
	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Absent
	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Provide subject matter expertise to website characterizations.	Absent
	Provide analyses and support for effectiveness assessment.	Absent
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Absent
	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Absent
	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Absent
	Provide input and assist in post-action effectiveness assessments.	Present
	Provide input and assist in the development of plans and guidance.	Present
	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Present
	Provide target recommendations which meet leadership objectives.	Absent
	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	Absent
	Report intelligence-derived significant network events and intrusions.	Present
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Absent

Mission Assessment Specialist	Provide expertise to course of action development.	Absent
	Provide subject matter expertise to the development of a common operational picture.	Absent
	Provide subject matter expertise to the development of cyber operations specific indicators.	Absent
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Absent
	Provide expertise to the development of measures of effectiveness and measures of performance.	Absent
	Assist in the identification of intelligence collection shortfalls.	Absent
	Brief threat and/or target current situations.	Absent
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Conduct end-of-operations assessments.	Absent
	Conduct in-depth research and analysis.	Absent
	Conduct nodal analysis.	Absent
	Conduct target research and analysis.	Absent
	Develop information requirements necessary for answering priority information requests.	Absent
	Develop measures of effectiveness and measures of performance.	Absent
	Develop munitions effectiveness assessment or operational assessment materials.	Absent
	Engage customers to understand customers' intelligence needs and wants.	Absent
	Estimate operational effects generated through cyber activities.	Absent
	Evaluate threat decision-making processes.	Absent
	Identify threat vulnerabilities.	Absent
	Generate requests for information.	Absent
	Identify intelligence gaps and shortfalls.	Absent
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Absent
	Monitor and report on validated threat activities.	Absent
	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Absent
	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Provide analyses and support for effectiveness assessment.	Absent
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Absent
	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Absent
	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Absent
	Provide input and assist in post-action effectiveness assessments.	Absent
	Provide input and assist in the development of plans and guidance.	Absent
	Provide effectiveness support to designated exercises, and/or time sensitive operations.	Absent

	Provide target recommendations which meet leadership objectives.	Absent
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Absent
Target Developer	Accurately characterize targets.	Absent
	Provide expertise to course of action development.	Absent
	Provide expertise to the development of measures of effectiveness and measures of performance.	Absent
	Build and maintain electronic target folders.	Absent
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Absent
	Conduct nodal analysis.	Absent
	Conduct target research and analysis.	Absent
	Coordinate target vetting with appropriate partners.	Absent
	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	Absent
	Determine what technologies are used by a given target.	Absent
	Develop all-source intelligence targeting materials.	Absent
	Develop measures of effectiveness and measures of performance.	Absent
	Develop munitions effectiveness assessment or operational assessment materials.	Absent
	Estimate operational effects generated through cyber activities.	Absent
	Evaluate available capabilities against desired effects to recommend efficient solutions.	Absent
	Generate requests for information.	Absent
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Absent
	Identify critical target elements.	Absent
	Initiate requests to guide tasking and assist with collection management.	Absent
	Maintain target lists (i.e., RTL, JTL, CTL, etc.).	Absent
	Perform targeting automation activities.	Absent
	Characterize websites.	Absent
	Produce target system analysis products.	Absent
	Provide aim point and reengagement recommendations.	Absent
	Provide analyses and support for effectiveness assessment.	Absent
	Provide input for targeting effectiveness assessments for leadership acceptance.	Absent
	Provide operations and reengagement recommendations.	Absent
	Provide target recommendations which meet leadership objectives.	Absent
	Provide targeting products and targeting support as designated.	Absent
	Provide time sensitive targeting support.	Absent
	Review appropriate information sources to determine validity and relevance of information gathered.	Absent
	Sanitize and minimize information to protect sources and methods.	Absent
	Support identification and documentation of collateral effects.	Absent
	Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.	Absent
Target Network Analyst	Provide expertise to course of action development.	Absent
	Classify documents in accordance with classification guidelines.	Absent

	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Absent
	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	Absent
	Identify and conduct analysis of target communications to identify information essential to support operations.	Absent
	Conduct nodal analysis.	Absent
	Conduct quality control to determine validity and relevance of information gathered about networks.	Absent
	Conduct target research and analysis.	Absent
	Determine what technologies are used by a given target.	Absent
	Apply analytic techniques to gain more target information.	Absent
	Generate and evaluate the effectiveness of network analysis strategies.	Absent
	Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)	Absent
	Generate requests for information.	Absent
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Absent
	Identify collection gaps and potential collection strategies against targets.	Absent
	Identify network components and their functionality to enable analysis and target development.	Absent
	Make recommendations to guide collection in support of customer requirements.	Absent
	Provide subject matter expertise to development of exercises.	Absent
	Perform content and/or metadata analysis to meet organization objectives.	Absent
	Profile targets and their activities.	Absent
	Provide target recommendations which meet leadership objectives.	Absent
	Review appropriate information sources to determine validity and relevance of information gathered.	Absent
	Reconstruct networks in diagram or report format.	Absent
	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.	Absent
Multi-Disciplined Language Analyst	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	Absent
	Determine what technologies are used by a given target.	Absent
	Identify collection gaps and potential collection strategies against targets.	Absent
	Make recommendations to guide collection in support of customer requirements.	Absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Advise managers and operators on language and cultural issues that impact organization objectives.	Absent
	Analyze and process information using language and/or cultural expertise.	Absent
	Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities.	Absent
	Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination.	Absent
	Conduct all-source target research to include the use of open source materials in the target language.	Absent
	Conduct analysis of target communications to identify essential information in support of organization objectives.	Absent

	Perform quality review and provide feedback on transcribed or translated materials.	Absent
	Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.	Absent
	Identify cyber threat tactics and methodologies.	Absent
	Identify target communications within the global network.	Absent
	Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis.	Absent
	Provide feedback to collection managers to enhance future collection and analysis.	Absent
	Perform foreign language and dialect identification in initial source data.	Absent
	Perform or support technical network analysis and mapping.	Absent
	Provide requirements and feedback to optimize the development of language processing tools.	Absent
	Perform social network analysis and document as appropriate.	Absent
	Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material.	Absent
	Tip critical or time-sensitive information to appropriate customers.	Absent
	Transcribe target voice materials in the target language.	Absent
	Translate (e.g., verbatim, gist, and/or summaries) target graphic material.	Absent
	Translate (e.g., verbatim, gist, and/or summaries) target voice material.	Absent
	Identify foreign language terminology within computer programs (e.g., comments, variable names).	Absent
	Provide near-real time language analysis support (e.g., live operations).	Absent
	Identify cyber/technology-related terminology in the target language.	Absent
All Source- Collection Manager	Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements.	Absent
	Analyze feedback to determine extent to which collection products and services are meeting requirements.	Absent
	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirements (e.g., duration, scope, communication requirements, interagency/international agreements).	Absent
	Assess and apply operational environment factors and risks to collection management process.	Present
	Assess performance of collection assets against prescribed specifications.	Present
	Compare allocated and available assets to collection demand as expressed through requirements.	Present
	Compile lessons learned from collection management activity's execution of organization collection objectives.	Absent
	Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.	Absent
	Construct collection plans and matrixes using established guidance and procedures.	Absent
	Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.	Absent
	Coordinate inclusion of collection plan in appropriate documentation.	Absent
	Re-task or re-direct collection assets and resources.	Absent

	Determine course of action for addressing changes to objectives, guidance, and operational environment.	Absent
	Determine existing collection management webpage databases, libraries and storehouses.	Absent
	Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function.	Present
	Determine organizations and/or echelons with collection authority over all accessible collection assets.	Present
	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	Present
	Develop coordinating instructions by collection discipline for each phase of an operation.	Absent
	Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis.	Absent
	Disseminate tasking messages and collection plans.	Absent
	Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems.	Absent
	Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures.	Absent
	Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.	Absent
	Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables.	Absent
	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	Absent
	Identify coordination requirements and procedures with designated collection authorities.	Absent
	Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.	Absent
	Identify potential collection disciplines for application against priority information requirements.	Absent
	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	Absent
	Issue requests for information.	Absent
	Link priority collection requirements to optimal assets and resources.	Absent
	Monitor completion of reallocated collection efforts.	Absent
	Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.	Absent
	Monitor the operational environment for potential factors and risks to the collection operation management process.	Absent
	Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements.	Absent
	Prioritize collection requirements for collection platforms based on platform capabilities.	Absent
	Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.	Absent

	Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures.	Absent
	Review capabilities of allocated collection assets.	Absent
	Review intelligence collection guidance for accuracy/applicability.	Absent
	Review list of prioritized collection requirements and essential information.	Absent
	Review and update overarching collection plan, as required.	Absent
	Revise collection matrix based on availability of optimal assets and resources.	Absent
	Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources.	Present
	Specify discipline-specific collections and/or taskings that must be executed in the near term.	Present
	Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.	Absent
All Source- Collection Requirements Manager	Analyze feedback to determine extent to which collection products and services are meeting requirements.	Absent
	Analyze incoming collection requests.	Absent
	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirements (e.g., duration, scope, communication requirements, interagency/international agreements).	Absent
	Assess efficiency of existing information exchange and management systems.	Absent
	Assess performance of collection assets against prescribed specifications.	Absent
	Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and adjust collection strategies and collection requirements accordingly.	Absent
	Close requests for information once satisfied.	Absent
	Collaborate with customer to define information requirements.	Absent
	Compile lessons learned from collection management activity's execution of organization collection objectives.	Absent
	Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.	Absent
	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	Absent
	Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.	Absent
	Disseminate reports to inform decision makers on collection issues.	Absent
	Conduct and document an assessment of the collection results using established procedures.	Absent
	Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.	Absent
	Evaluate extent to which collected information and/or produced intelligence satisfy information requests.	Absent
	Evaluate extent to which collection operations are synchronized with operational requirements.	Absent
	Evaluate the effectiveness of collection operations against the collection plan.	Absent
	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	Absent

	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	Absent
	Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.	Absent
	Issue requests for information.	Absent
	Modify collection requirements as necessary.	Absent
	Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.	Absent
	Review capabilities of allocated collection assets.	Absent
	Review intelligence collection guidance for accuracy/applicability.	Absent
	Review list of prioritized collection requirements and essential information.	Absent
	Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.	Absent
	Submit information requests to collection requirement management section for processing as collection requests.	Absent
	Track status of information requests, including those processed as collection requests and production requirements, using established procedures.	Absent
	Translate collection requests into applicable discipline-specific collection requirements.	Absent
	Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness.	Absent
	Validate requests for information according to established criteria.	Absent
Cyber Intel Planner	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.	Absent
	Coordinate for intelligence support to operational planning activities.	Absent
	Assess all-source intelligence and recommend targets to support cyber operation objectives.	Absent
	Assess target vulnerabilities and/or operational capabilities to determine course of action.	Absent
	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Absent
	Assist in the development and refinement of priority information requirements.	Absent
	Enable synchronization of intelligence support plans across partner organizations as required.	Absent
	Provide input to the identification of cyber-related success criteria.	Absent
	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).	Absent
	Contribute to crisis action planning for cyber operations.	Absent
	Contribute to the development of the organization's decision support tools if necessary.	Absent
	Incorporate intelligence equities into the overall design of cyber operations plans.	Absent
	Coordinate with intelligence planners to ensure that collection managers receive information requirements.	Absent
	Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks.	Absent
	Coordinate, produce, and track intelligence requirements.	Absent

	Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans.	Absent
	Use intelligence estimates to counter potential target actions.	Absent
	Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.	Absent
	Develop and review intelligence guidance for integration into supporting cyber operations planning and execution.	Absent
	Develop detailed intelligence support to cyber operations requirements.	Absent
	Develop potential courses of action.	Absent
	Develop, implement, and recommend changes to appropriate planning procedures and policies.	Absent
	Draft cyber intelligence collection and production requirements.	Absent
	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	Absent
	Evaluate intelligence estimates to support the planning cycle.	Absent
	Evaluate the conditions that affect employment of available cyber intelligence capabilities.	Absent
	Incorporate intelligence and counterintelligence to support plan development.	Absent
	Identify all available partner intelligence capabilities and limitations supporting cyber operations.	Absent
	Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.	Absent
	Identify cyber intelligence gaps and shortfalls for cyber operational planning.	Absent
	Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.	Absent
	Provide input to or develop courses of action based on threat factors.	Absent
	Interpret environment preparations assessments to determine a course of action.	Absent
	Issue requests for information.	Absent
	Lead and coordinate intelligence support to operational planning.	Absent
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Absent
	Maintain situational awareness to determine if changes to the operating environment require review of the plan.	Absent
	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
	Prepare for and provide subject matter expertise to exercises.	Absent
	Provide cyber focused guidance and advice on intelligence support plan inputs.	Absent
	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	Absent
	Review and comprehend organizational leadership objectives and guidance for planning.	Absent
	Scope the cyber intelligence planning effort.	Absent
	Document lessons learned that convey the results of events and/or exercises.	Absent
Cyber Ops Planner	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	Absent
	Evaluate intelligence estimates to support the planning cycle.	Absent

	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Absent
	Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.	Absent
	Incorporate cyber operations and communications security support plans into organization objectives.	Absent
	Identify cyber intelligence gaps and shortfalls for cyber operational planning.	Absent
	Integrate cyber planning/targeting efforts with other organizations.	Absent
	Interpret environment preparations assessments to determine a course of action.	Absent
	Issue requests for information.	Absent
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Absent
	Maintain situational awareness of cyber-related intelligence requirements and associated tasking.	Absent
	Maintain situational awareness of partner capabilities and activities.	Absent
	Maintain situational awareness to determine if changes to the operating environment require review of the plan.	Absent
	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	Absent
	Prepare for and provide subject matter expertise to exercises.	Absent
	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	Absent
	Provide input to the administrative and logistical elements of an operational support plan.	Absent
	Provide planning support between internal and external partners.	Absent
	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	Absent
	Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.	Absent
	Submit or respond to requests for deconfliction of cyber operations.	Absent
	Document lessons learned that convey the results of events and/or exercises.	Absent
Partner Integration Planner	Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.	Absent
	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Absent
	Provide expertise to course of action development.	Absent
	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).	Absent
	Contribute to crisis action planning for cyber operations.	Absent
	Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers.	Absent
	Coordinate with intelligence and cyber defense partners to obtain relevant essential information.	Absent

	Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations.	Absent
	Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives.	Absent
	Develop strategy and processes for partner planning, operations, and capability development.	Absent
	Develop, implement, and recommend changes to appropriate planning procedures and policies.	Absent
	Develop, maintain, and assess cyber cooperation security agreements with external partners.	Absent
	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Absent
	Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community.	Absent
	Identify and manage security cooperation priorities with external partners.	Absent
	Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.	Absent
	Integrate cyber planning/targeting efforts with other organizations.	Absent
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Absent
	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Absent
	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	Absent
	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	Absent
	Propose policy which governs interactions with external coordination groups.	Absent
	Prepare for and provide subject matter expertise to exercises.	Absent
	Provide cyber focused guidance and advice on intelligence support plan inputs.	Absent
	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	Absent
	Provide planning support between internal and external partners.	Absent
	Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations.	Absent
	Serve as a liaison with external partners.	Absent
	Submit or respond to requests for deconfliction of cyber operations.	Absent
	Synchronize cyber international engagement activities and associated resource requirements as appropriate.	Absent
	Synchronize cyber portions of security cooperation plans.	Absent
	Document lessons learned that convey the results of events and/or exercises.	Absent
Cyber Operator	Analyze internal operational architecture, tools, and procedures for ways to improve performance.	Absent
	Analyze target operational architecture for ways to gain access.	Absent
	Collaborate with development organizations to create and deploy the tools needed to achieve objectives.	Absent

	Conduct access enabling of wireless computer and digital networks.	Present
	Conduct collection and processing of wireless computer and digital networks.	Present
	Conduct exploitation of wireless computer and digital networks.	Present
	Conduct network scouting and vulnerability analyses of systems within a network.	Absent
	Conduct on-net activities to control and exfiltrate data from deployed technologies.	Absent
	Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies.	Absent
	Conduct open source data collection via various online tools.	Absent
	Conduct survey of computer and digital networks.	Absent
	Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).	Absent
	Detect exploits against targeted networks and hosts and react accordingly.	Absent
	Develop new techniques for gaining and keeping access to target systems.	Absent
	Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.	Absent
	Exploit network devices, security devices, and/or terminals or environments using various methods or tools.	Absent
	Facilitate access enabling by physical and/or wireless means.	Present
	Identify potential points of strength and vulnerability within a network.	Present
	Maintain situational awareness and functionality of organic operational infrastructure.	Present
	Operate and maintain automated systems for gaining and maintaining access to target systems.	Absent
	Conduct cyber activities to degrade/remove information resident in computers and computer networks.	Absent
	Process exfiltrated data for analysis and/or dissemination to customers.	Absent
	Provide real-time actionable geolocation information.	Absent
	Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.	Absent
Cyber Crime Investigator	Test and evaluate locally developed tools for operational use.	Absent
	Test internal developed tools and techniques against target tools.	Absent
	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.	Absent
	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.	Absent
	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).	Absent
	Examine recovered data for information of relevance to the issue at hand.	Absent
	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.	Absent
	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.	Absent
	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.	Absent
	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Absent
	Identify elements of proof of the crime.	Absent

	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.	Absent
	Process crime scenes.	Absent
	Secure the electronic device or information source.	Absent
	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Absent
	Analyze the crisis to ensure public, personal, and resource protection.	Absent
	Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.	Absent
	Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.	Absent
	Provide criminal investigative support to trial counsel during the judicial process.	Absent
	Analyze computer-generated threats for counter intelligence or criminal activity.	Absent
	Gather and preserve evidence used on the prosecution of computer crimes.	Absent
	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.	Absent
	Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes.	Absent
	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).	Absent
	Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.	Absent
	Prepare reports to document the investigation following legal standards and requirements.	Absent
Law Enforcement /Counter Intelligence Forensics Analyst	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.	Present
	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).	Present
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Present
	Analyze incident data for emerging trends.	Absent
	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Absent
	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	Absent
	Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.	Present
	Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	Present
	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Present
Cyber Defense Forensics Analyst	Analyze organizational cyber policy.	Present
	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.	Present
	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.	Absent

Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.	Absent
Decrypt seized data using technical means.	Absent
Provide technical summary of findings in accordance with established reporting procedures.	Absent
Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	Absent
Examine recovered data for information of relevance to the issue at hand.	Absent
Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Absent
Perform dynamic analysis to boot an "image" of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.	Absent
Perform file signature analysis.	Absent
Perform hash comparison against established database.	Present
Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).	Present
Perform timeline analysis.	Present
Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	Present
Perform static media analysis.	Absent
Perform tier 1, 2, and 3 malware analysis.	Absent
Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	Absent
Provide technical assistance on digital evidence matters to appropriate personnel.	Absent
Recognize and accurately report forensic artifacts indicative of a particular operating system.	Absent
Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).	Absent
Capture and analyze network traffic associated with malicious activities using network monitoring tools.	Absent
Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Absent
Conduct cursory binary analysis.	Absent
Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Absent
Perform virus scanning on digital media.	Absent
Perform file system forensic analysis.	Absent
Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).	Absent
Perform static malware analysis.	Absent
Utilize deployable forensics toolkit to support operations as necessary.	Absent
Coordinate with intelligence analysts to correlate threat assessment data.	Present
Process image with appropriate tools depending on analyst's goals.	Present
Perform Windows registry analysis.	Absent

	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Absent
	Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.	Absent
	Correlate incident data and perform cyber defense reporting.	Absent
	Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.	Present
	Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Absent
	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	Absent
	Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.	Absent

List of Potential threats at Autumn-CSTL that could exploit vulnerabilities for critical assets due to missing cybersecurity specialty areas, Cybersecurity work roles and Cybersecurity tasks:

Threats
Loss of Confidentiality, Integrity, Availability
Loss of Data Privacy
Sensitive Information Leak
Non-compliance Issues and Fines
Unauthorized Access
Unauthorized modification
Disruption of Service

List of Potential risks for Autumn-CSTL due to missing Cybersecurity Specialty Areas, Cybersecurity work roles and Cybersecurity tasks

Risks
Lack of the security policies and prevention controls can lead to a security breach
Due to the unavailability of solid business continuation plans, it can be difficult to recover from an interruption of operations situation which can also stand in the way of the company meeting its goals
Non-compliance issues all over the company can lead to various issues and heavy fines
Absence of stronger IDS and IPS can lead to a network based attack
Absence of detective and preventive controls on the systems and servers can lead to a malware attack
There can be danger to the privacy of data
Because of inaccurately configured systems, it is possible to give someone unauthorized access

List of recommended policies (Hiring new Cybersecurity staff, Educating current staff, outsourcing) for each recommended cybersecurity specialty area, cybersecurity work role, or cybersecurity task that should be created to mitigate the identified risks (It is not required to write detailed policies)

- Regular audits must be conducted and monitor logs must be maintained so as to assess the security standing of the company
- An incident response playbook must be created and updated so as to contact the incident handling team when an event occurs.
- Senior management and board must document and plan a Business continuity and a disaster recovery plan so that no crucial time is wasted during an actual crisis
- Separation of duties and the least privilege principle must be implemented company wide
- A thorough risk assessment must be performed periodically so that it is easy to keep track of the security needs the company might have.
- More cybersecurity staff must be hired according to the NICE Cybersecurity work force so that the data and functions of the company stay secure.
- Compliance audits must be scheduled every few months to avoid clash with the government and suffer heavy fines.

Part C : Security Risk Management Recommendations

Provide The List of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits based on your risk management analysis

For HGA:

- Implementing access controls will ensure the integrity and confidentiality of critical data, which is a must for HGA as it deals with many financial assets.
- Using more robust encryption strategies will ensure confidentiality inside the communications of HGA
- Better authentication will consist of implementing stronger passwords, MFA (multifactor authentication), and addition OTPs
- SIEM (Security Information and Event Management) should be used for centralizing the auditing and logging practices inside HGA for better Intrusion detection and accountability.
- Under operational controls, HGA should raise more security awareness and conduct security training workshops for not only the employees of HGA but as well the higher-ups.
- They should also make incident reporting and incident handling strategies better and more through while also updating their incident response playbook significantly
- Data should be encrypted in transit as well as when it is at rest with industry standard algorithms to prevent information leak.
- HGA must conduct regular audits and security risks assessments to be on top of the threats that might follow in the future.

For Autumn-CSTL:

- Data encryption should happen on both client and server side, both when it is stored and while it is being moved around, to prevent illegal access and manipulation.
- Limiting access to sensitive data by putting in place access control methods such as complex passwords, two-factor authentication, and access control lists can help a lot with unauthorized access problems.
- Implement data encryption, implement access controls and authentication, and implement regular security assessments and audits.
- Implement redundancy and failover mechanisms, implement disaster recovery and business continuity plans, and implement backup and recovery procedures.
- Implement compliance policies and procedures, regularly review and update compliance measures, and conduct regular audits.
- Regularly review and update business objectives and strategies, implement business continuity plans, and conduct regular risk assessments and audits.
- Implement anti-virus and anti-malware software, regularly update software and operating systems, and implement application whitelisting and patch management procedures.

Provide the total cost benefit in \$ for the recommended controls, methods and policies based on your security risks management analysis in Parts A and B above

For HGA:

- Residual risk with current controls: \$1,480,000
- Residual Risk with new controls: \$300,000
- Proposed Security Budget: \$800,000

Residual Risk = Risk with current controls – Risk with new controls

$$\$1,480,000 - \$300,000 = \$1,180,000$$

In this case, the value of risk reduction exceeds the budget of the proposed controls.

- Cost Benefit ratio analysis for Mixed strategy Budget
Proposed Security Risk Budget Cost/ Expected security risk-benefit
 $\$800,000/\$1,180,000 = 0.677$

For Autumn-CSTL:

- Residual Risk with current controls: \$1,700,000
- Residual Risk with new controls: \$340,000
- Proposed Security Budget: \$800,000

Residual Risk = Risk with current controls – risk with new controls

$$\$1,700,000 - \$340,000 = \$1,360,000$$

In this case, the value of risk reduction exceeds the budget of the proposed controls.

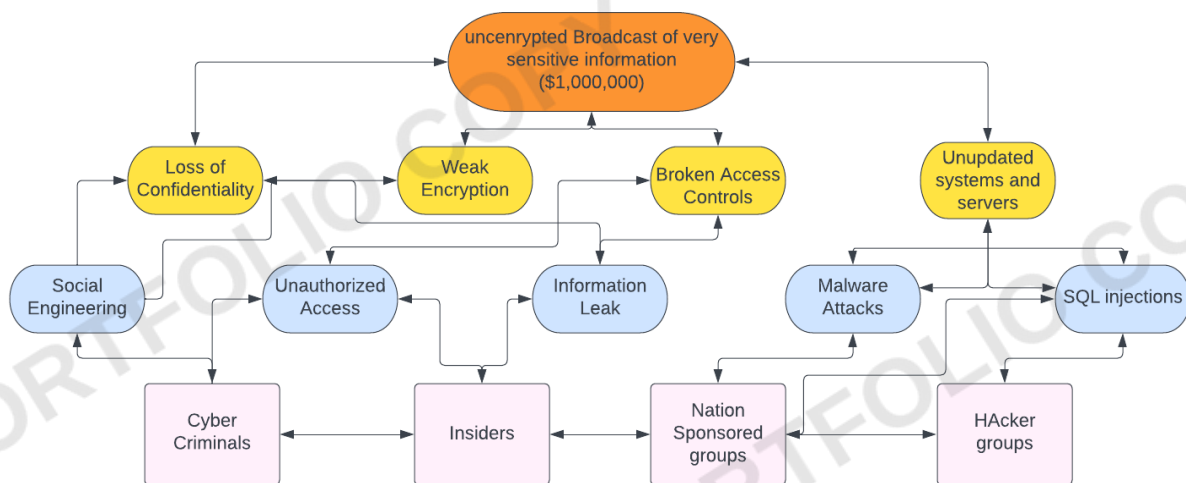
- Cost Benefit ratio analysis for Mixed strategy Budget
Proposed Security Risk Budget Cost/ Expected security risk-benefit
 $\$800,000/\$1,360,000 = 0.588$

Comparing the proposed security controls, methods and policies budget for HGA with the proposed security controls, methods and policies budget for Autumn-CSTL:

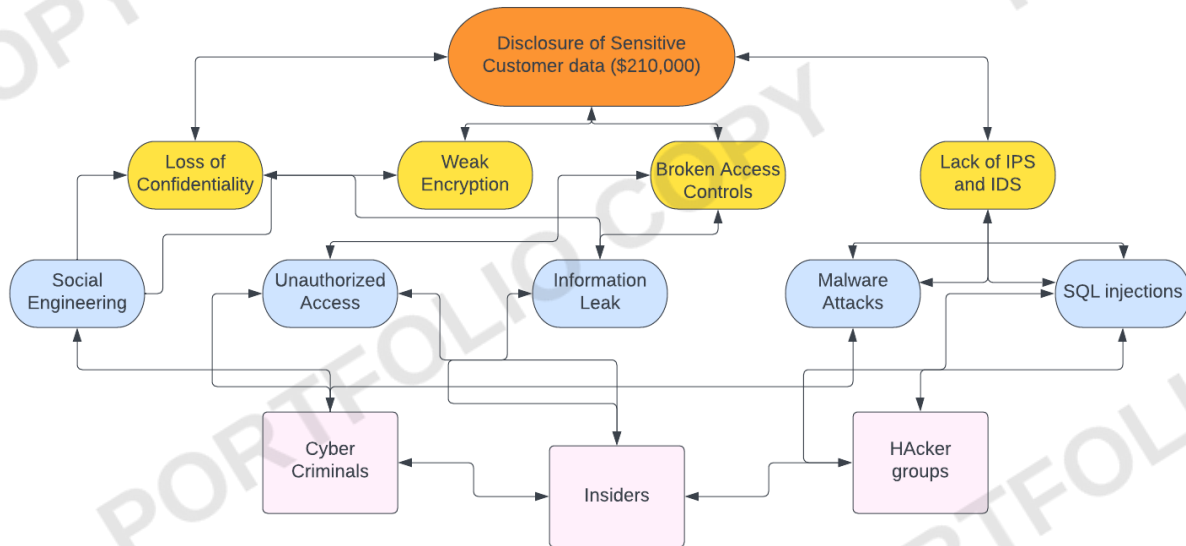
Points of Consideration	HGA	Autumn-CSTL
Industry	Financial - Government	Private – Technology Solutions
Mission	Manages Financial services for various government agencies	Has a through R&D department that makes tech solutions and they also provide tech consultation

Geographic Presence	United States Of America	Pune, India and USA
Number of Employees	1000	2800
Network Topology	Appendix 3	Appendix 4
Critical assets in \$	\$2,197,000	\$2,580,000
Threat Environment	Nation State, Competitors, Hacker Organizations	Nation State, Competitors, Hacker organizations, Insider threat
Threat Agents	Cyber Criminals, Insiders, Hacker Groups, Nation Sponsored groups	Cyber criminals, Hacker groups, Insiders
Residual Security Risk in \$	\$1,180,000	\$1,360,000
Total Budget for risk Prevention and response controls, methods, policies	\$800,000	\$800,000
Security Budget/ \$ security risk improvement	0.677	0.588
Security Budget/ \$ Critical assets	0.318	0.287
Security budget/ \$ employee	880	312

Attack Tree for Hypothetical Government Agency (HGA):



Attack Tree for Autumn-CSTL:



Vulnerabilities and Exploitation Probabilities:

For HGA:

Vulnerability	Exploitation Probability
Falsified Time Sheets	45
Outdated passwords	50
Unauthorized access to confidential information	35
Corruption of data	10
Loss of data	15
Deletion of critical data	20
Access to master database	35
Unencrypted servers	20
Unauthorized modification of critical data	40
Lack of security policies	20

For Autumn-CSTL:

Vulnerability	Exploitation Probability
Weak Authentication	25
Unauthorized access	30
Social Engineering	45
Equipment failure	30
Weak Access Control	20
Information theft	10

Denial of Service	25
Firewall Misconfiguration	10
Equipment failure	15
Network Infrastructure attack	10
Database attacks	30

Cybersecurity Workforce Recommendation:

FOR HGA:

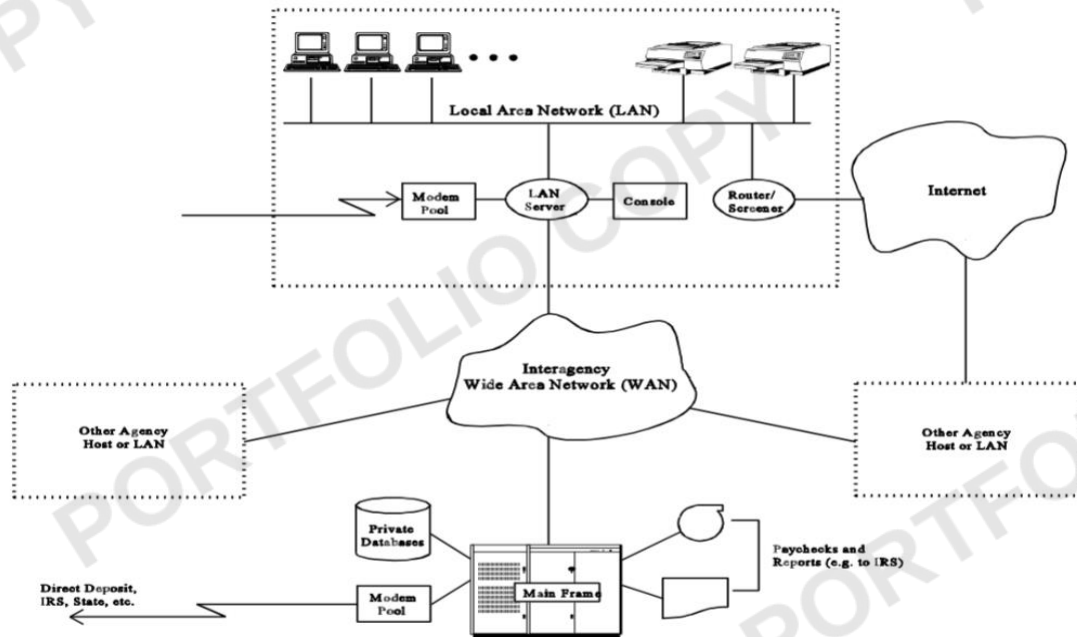
- HGA should perform periodic security assessments and audits to be on top of security risks
- Regular audits must be conducted and monitor logs must be maintained so as to assess the security standing of the company
- An incident response playbook must be created and updated so as to contact the incident handling team when an event occurs.
- Senior management and board must document and plan a Business continuity and a disaster recovery plan so that no crucial time is wasted during an actual crisis
- Separation of duties and the least privilege principle must be implemented company wide

For Autumn-CSTL:

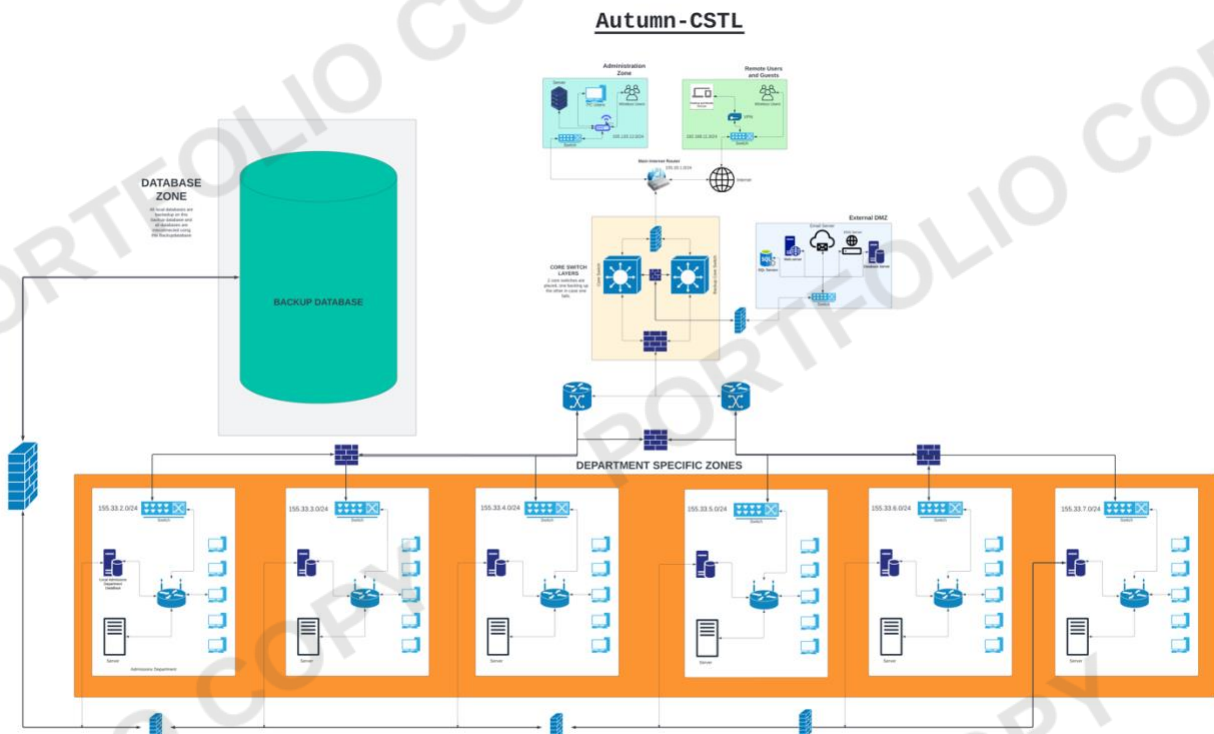
- A through risk assessment must be performed periodically so that it is easy to keep track of the security needs the company might have.
- More cybersecurity staff must be hired according to the NICE Cybersecurity work force so that the the data and functions of the company stay secure.
- Compliance audits must be scheduled every few months to avoid clash with the government and suffer heavy fines.
- Implement redundancy and failover mechanisms, implement disaster recovery and business continuity plans, and implement backup and recovery procedures.
- Implement compliance policies and procedures, regularly review and update compliance measures

Part D: Appendix

Appendix 3: Detailed network topology of HGA



Appendix 4: Detailed network topology of Autumn-CSTL



Being a Startup, Autumn-CSTL has given me their last version of network infrastructure for privacy concerns. As we can see in the above network architecture, they have separated departments inside the organization in a separate zone with their private database. A backup database also stores the information from all those private databases. This was a big vulnerability in this version of their architecture. They do have a designated DMZ and VPN capabilities for remote employees if needed. The entire architecture is filled with backup complements like a backup database, switch, and firewalls, making it harder to manage. The organization was on this architecture for a little above 3 years. All the internet traffic in the network is heavily monitored to avoid data leakage. Overall, having separate zones and data segregation was a strong point for the organization's cybersecurity needs.

References:

- <https://www.techtarget.com/searchsecurity/definition/role-based-access-control-RBAC>
- <https://www.digitalguardian.com/blog/what-role-based-access-control-rbac-examples-benefits-and-more>
- <https://www.scaler.com/topics/database-users-in-dbms/>
- <https://security.berkeley.edu/education-awareness/database-hardening-best-practices>
- <https://www.navisite.com/blog/what-is-database-hardening/>
- https://blog.netwrix.com/2022/12/21/database_security_hardening/
- <https://www.actian.com/a-guide-to-managing-data-risks/>
- <https://www.gdpreu.org/the-regulation/key-concepts/personal-data/>
- <https://oag.ca.gov/privacy/ccpa>
- <https://www.itgovernance.co.uk/iso27001>
- **SANS Remote Access Policy:**
<https://northeastern.instructure.com/courses/123529/modules/items/7392109>
- **SANS Routers and Switch Security Policy :**
<https://northeastern.instructure.com/courses/123529/modules/items/7392133>
- **SANS Virtual Private Network Policy :**
<https://northeastern.instructure.com/courses/123529/modules/items/7392158>
- **SANS Remote Access Tools Policy:**
<https://northeastern.instructure.com/courses/123529/modules/items/7392159>
- **SANS Database_credentials_Policy:**
<https://northeastern.instructure.com/courses/123529/modules/items/7392180>
- **SANS Web Application Security Policy:**
<https://northeastern.instructure.com/courses/123529/modules/items/7392205>
- **SANS Wireless Communication Standard :**
<https://northeastern.instructure.com/courses/123529/modules/items/7392228>
- **SANS Wireless Communication Policy:**
<https://northeastern.instructure.com/courses/123529/modules/items/7392229>
- <https://www.cisa.gov/ncas/tips/ST05-003>
- <https://securitygladiators.com/secure-wireless-network/>
- https://media.defense.gov/2020/Aug/18/2002479461/-1/-1/0/HARDENING_NETWORK_DEVICES.PDF
- <https://informationsecurityprogram.com/wireless-access-security-policy-best-practices/>
- <https://informationsecurityprogram.com/wireless-access-security-policy-best-practices/>