CLASS 5200: SECURITY RISK MANAGEMENT AND ASSESSMENT

APRIL 28, 2022

NAME: SHREYA PATIL

NUID: 001507392

PART – A SECURITY RISK MANAGEMENT ASSESSMENT

EXECUTIVE SUMMARY

Information System Name: Hypothetical Government Agency

Information System Categorization:

Assets	Information Security Elements		
	Confidentiality	Integrity	Availability
Financial Resources	High	High	High
PC'S	High	High	High
Printers	Medium	Medium	Medium
LAN Server	High	High	High
Modem Pool	High	High	High
Special Console	High	High	High
Router	High	High	High
Personnel Information	High	High	High
Contracting Documents	High	High	Medium
Draft Regulations	High	High	High
Internal Correspondence	Medium	Medium	Medium
Business Documents	High	High	High
Reputation (Intangible)	High	High	High
Employee Confidence	High	High	High

Organization Name: Hypothetical Government Agency

Organization Address: 281 Park Ave, New York, New York 10017

Brian Robinson
Tittle: Chief Executive Officer
Email: brobinson@hga.com
Phone: 660-756-8907

Sean Randles
Tittle: Chief Operating Officer
Email: srandle@hga.com
Phone: 660-756-8918

Jeff Sykes
Tittle: Chief Information Officer
Email: jsykes@hga.com
Phone: 660-756-8901

Sashank Narain
Tittle: Chief Financial Officer
Email: snarain@hga.com

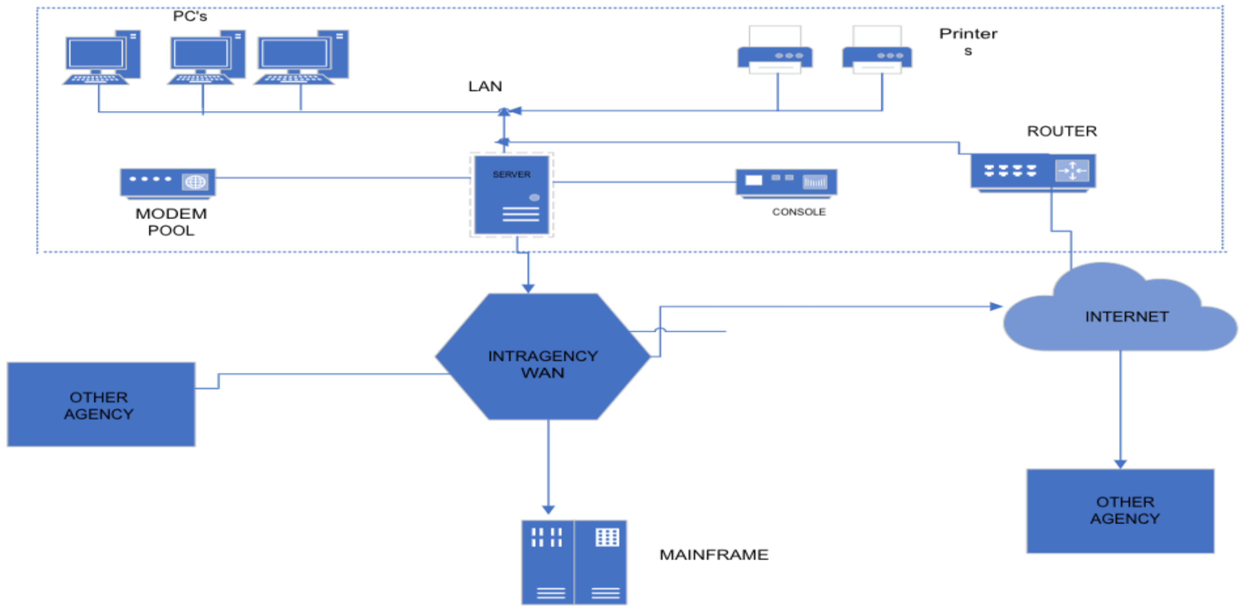
Phone: 660-756-8903

Information System Operational Status: Operational

Information System Type: Major Application

System Description: Funds Transferred from US Government to individual customers

System Environment:



The network topology describes the distributed system architecture of HGA. This diagram helps in identifying and scoping the assets owned by HGA which are going to be evaluated in the security risk analysis. It also helps in identifying the neighboring assets, their ownership and potential risks posed by such. As seen in the network diagram the LAN server acts as the central component of the architecture. As the router, printers, computers, modem pool and special console are directly being connected to the LAN server.

Interconnection of System Information:

System Name: Hypothetical Government Agency

Type of Organization: Public Sector Telecommunication industry

Type of Contract: Government Contract

Date: May 27, 2007

FIPS 199 Category: High

C&A category: Accredited and certified

Authorizing Individual:

APPLICABLE LAWS/ FRAMEWORKS/ STANDARDS/ POLICIES/ REGULATIONS:

Federal Trade Commission Safeguards rule
Federal Information Security Management Act of 2002
ISO 20022
ISO 22301- Security and Resilience- Business Continuity Management Systems
ISO 27001- Information Security Management System
US Privacy act of 1974

Minimum Security Controls:

Security Control	**Observation**	**Status**	**Content type**	**Responsible Authority**
Review of Security Controls (MOT1)	The security controls were satisfactorily reviewed	Completed	Common	CIO
LAN Server Access specific policy (MOT2)	Access controls to LAN were made stronger and accordingly documented.	Completed	Common	CISO
Storage of sensitive information policy (MOT3)	Policies relting to sensitive information were identified	Partial	Common	CIO
Authorize Processing (Certification and Accreditation) (MOT4)	Formal Process for authorization is being drafted.	Partial	Common	CIO
Physical Security (MOT5)	Effectiveness of controls were reviewed.	Completed	Common	CISO
Criminal History Check requirement (MOT6)	Criminal check process and policies are being drafted	Partial	Common	CISO

Security Awareness Training related to critical system specific issues requirement (MOT7)	Frequency of Security Training has been increased	Completed	Common	CIO
Backup services (MOT8)	Regular backups are scheduled	Completed	Common	CIO
Incident Response Capability (MOT9)	Policies relating to Incident Response were identified	Partial	Common	CIO
Documentation of using Removable Media (MOT10)	Removable media usage policies are being drafted	Partial	Common	CISO
Periodic maintenance and patch management (MOT11)	Policies and controls are being drafted	Partial	Common	CISO
Data Integrity (MOT12)	Effectiveness of controls were reviewed.	Completed	Common	CIO
Strong I&A Systems (MOT13)	Effectiveness of controls were reviewed.	Completed	Common	CIO
Installation of Unified Threat Management services (MOT14)	Policies and controls are being drafted	Partial	Common	CIO
Audit Trails (MOT15)	Policies relating to audit trails were identified	Completed	Common	CIO

Information Security Plan Completion Date: 2/20/22
Information Security Plan Approval Date: 2/20/22

ASSETS:

The following is the Information Assets Inventory :

ASSET	ASSET NAME	ASSET Value
A1	FINANCIAL RESOURCES	1,000,000
A2	PC'S	300*150=45000
A3	Printers	350*20= 7000
A4	LAN Server	55000
A5	Modem Pool	850
A6	Special Console	3000
A7	Router	50000
A8	Personnel Information	35000
A10	Contracting and Procurement Documents	18000
A11	Draft Regulations	15000
A12	Internal Correspondence	15000
A13	Day to Day Business Documents	25000
A14	Reputation (Intangible)	75,000
A15	Employee Confidence (Intagible)	100,000
A16	VPN Server	30,000
A17	DMZ	4,000

THREATS:

The following are the list of threats based on HGA case:

Threat Number	Threat Name
T1	Payroll Fraud
T2	Payroll Errors
T3	Interruption of operations
T4	Disclosure or Brokerage of Info
T5	Network- Related attacks

VULNERABILITIES:

The following are the list of vulnerabilities based on HGA case:

Vulnerability Number	Vulnerability Name
V1	Falsified time sheets
V2	Unauthorized Access
V3	Bogus Time and Attendance Applications
V4	Unauthorized Modifications of Time and attendance Sheets
V5	Vulnerabilities related to Payroll Errors
V6	Vulnerabilities related to Continuity of Operations
V7	COG Contingency Planning
V8	Division Contingency Planning

V9	Virus Prevention
V10	Accidental Corruption and Loss of Data
V11	Vulnerabilities Related to disclosure or brokerage of information
V12	vulnerabilities related to Network Related attacks

CURRENT SECURITY CONTROLS AND POLICIES:

SECURITY CONTROLS	SECURITY CONTROLS NAME
S1	General Use and Administration of HGA's Computer System
S2	Protection Against Payroll Fraud & Errors-Time & Attendance Application
S3	Protection Against Unauthorized Execution
S4	Protection Against Payroll errors
S5	Protection Against Accidental Corruption or Loss of Payroll Data
S6	Protection Against Interruption of Operations
S7	COG Contingency Planning
S8	Division Contingency Planning
S9	Protection Against Disclosure or Brokerage of Information
S10	Protection Against Network Related Threats
S11	Protection Against Risks from Non- HGA Computer Systems

NEW CONTROLS PROVIDED BY CISO:

Proposed Security Controls	Security Controls Name
P1	one-time passwords for Time and Attendance Clerks
P2	digital signatures by using smart tokens
P3	quarterly compliance audit reports
P4	additional contingency plan training
P5	courier-delivered magnetic tapes for WAN outages
P6	regular backup services for about 5 percent of HGA's PCs
P7	improvement of security awareness training
P8	hard-disk encryption utilities
P9	regular review the mainframe audit log
P10	installing "screen lock" software on PCs
P11	restricted version of the mail utility be provided for dial-in
P12	replace current modem pool with encrypting modems

Subset of Assets:

Asset Number	Asset Name	Asset Value
A1	Financial Resources	1,000,000
A4	LAN Server	55,000
A7	Router	50,000
A8	Personnel Information	35,000

Subset of Threats:

Threat Number	Threat Name
T1	Payroll Fraud
T3	Interruption of operations
T4	Disclosure or Brokerage of Info
T5	Network- Related attacks

Subset of Vulnerabilities:

Vulnerability Number	Vulnerability Name
V2	Unauthorized Access
V9	Virus Prevention
V11	Vulnerabilities Related to disclosure or brokerage of information
V12	Vulnerabilities related to Network Related Attacks

Threat/ Vulnerabilities pairs

	T1	T3	T4	T5
V2	95	80	90	90
V9	90	95	95	90
V11	90	85	95	80
V12	90	90	85	95

Total Threat= 1,435

1. Due to the System’s infrastructure and weak I&A system of HGA, Unauthorized Access is one of the most critical vulnerabilities. As this vulnerability may exploit assets with greater values, it has been assigned with higher probabilities in the given matrix.
2. Virus Contamination poses a significant risk and may impact a lot of critical operations of an organization. Due to lack of adherence to virus-prevention procedures and weak Server Access Controls, probabilities of virus contamination have been assigned with greater probabilities in the given matrix.
3. The present system infrastructure holding critical information of employees has potential vulnerabilities related to disclosure or brokerage of information. Also due to lack of secure storage of payroll information and eavesdropping into the conversations of other users with LAN Server pose significant threats to HGA’s critical information assets.

4. As there is no authentication required for dial-in conversations, and no controls for sending accessing critical information via dialing-in, vulnerabilities related to Network Related Attacks is assigned with assigned with higher probabilities in the given matrix.

Asset/ Vulnerabilities pairs

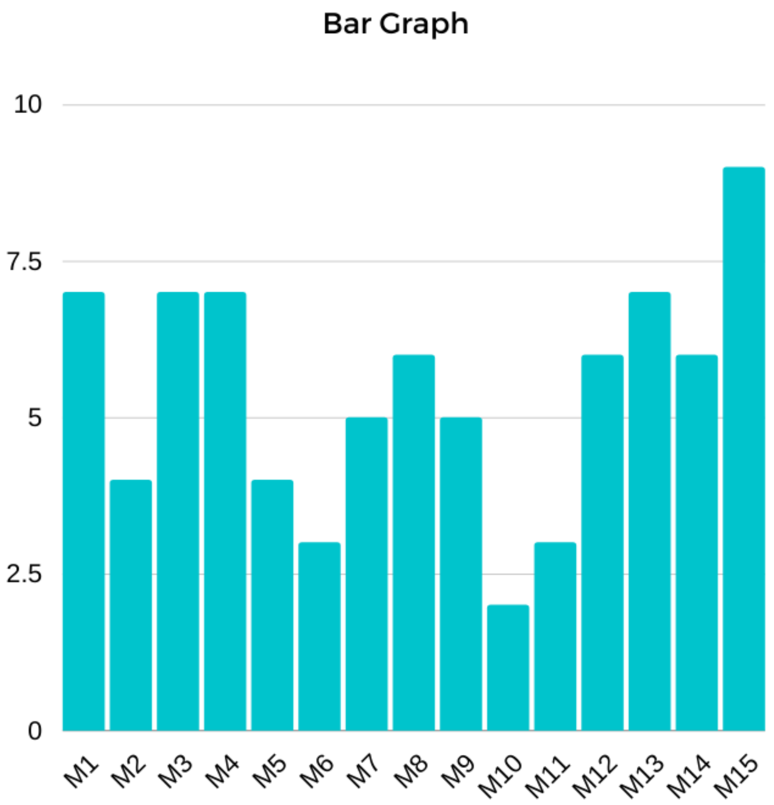
Assets	Vulnerabilities
A1-Financial Resources	V2- Unauthorized Access
	V9- Virus Prevention
	V11-Vulnerabilities Related to disclosure or brokerage of information
A4-LAN Server	V2- Unauthorized Access
	V12- Vulnerabilities related to Network Related Attacks
A7-Router	V9- Virus Prevention
	V12- Vulnerabilities related to Network Related Attacks
A8-Personnel Information	V2- Unauthorized Access
	V11-Vulnerabilities Related to disclosure or brokerage of information

The following is a list of various Risk Management Controls.

Managerial	**Operational**	**Technical**
Review of Security Controls (MOT1)	Physical Security (MOT5)	Strong I&A Systems (MOT13)
LAN Server Access specific policy (MOT2)	Criminal History Check requirement (MOT6)	Installation of Unified Threat Management services (MOT14)
Storage of sensitive information policy (MOT3)	Security Awareness Training related to critical system specific issues requirement (MOT7)	Audit Trails (MOT15)
Authorize Processing (Certification and Accreditation) (MOT4)	Backup services (MOT8)	
	Incident Response Capability (MOT9)	
	Documentation of using Removable Media (MOT10)	
	Periodic maintenance and patch management (MOT11)	
	Data Integrity (MOT12)	

Comparison of Security Control in place for HGA with Risk Management Controls.

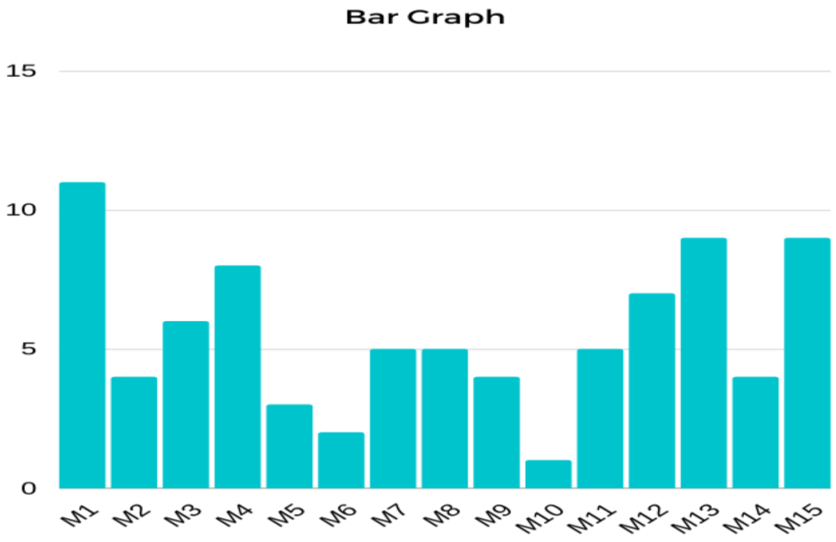
SECURITY CONTROLS	SECURITY CONTROLS NAME	Risk Management Controls. (MOT)
S1	General Use and Administration of HGA’s Computer System	1,4,3,7,8,11,13,15
S2	Protection Against Payroll Fraud & Errors-Time & Attendance Application	3,4,6,8,9,12,14
S3	Protection Against Unauthorized Execution	1,4,5,8,10,13,15
S4	Protection Against Payroll errors	1,3,4,7,12,13,14,15
S5	Protection Against Accidental Corruption or Loss of Payroll Data	1,2,8,9,12,14,15
S6	Protection Against Interruption of Operations	1,2,3,5,9,11,13,15
S7	COG Contingency Planning	1,3,4,8,9,12,15
S8	Division Contingency Planning	1,2,3,4,6,7,12,13
S9	Protection Against Disclosure or Brokerage of Information	1,3,5,6,7,12,13,14,15
S10	Protection Against Network Related Threats	1,2,7,8,10,12,13,14,15
S11	Protection Against Risks from Non- HGA Computer Systems	1,4,7,9,11,13,14,15



Comparison of Security Control recommended by CISO with Risk Management Controls.

Proposed Security Controls	Security Controls Name	
P1	one-time passwords for Time and Attendance Clerks	1, 4, 12, 13, 14, 15
P2	digital signatures by using smart tokens	4, 11,12, 14,15
P3	quarterly compliance audit reports	1,4,11,12
P4	additional contingency plan training	1,2,4,12,13,15
P5	courier-delivered magnetic tapes for WAN outages	1,3,4,7,8,9,13,15
P6	regular backup services for about 5 percent of HGA's PCs	1,3,4,7,8,9,11,13,14
P7	improvement of security awareness training	1,3, 4,6,7,11,13,15
P8	hard-disk encryption utilities	1,2,7,8,11,12,15
P9	regular review the mainframe audit log	1,4,5,9,12,13,15
P10	installing "screen lock" software on PCs	1,3,5, 7,8,12,13,15
P11	restricted version of the mail utility be provided for dial-in	1,2,3,5,7,12,13

P12	replace current modem pool with encrypting modems	1,2,3,8,9,12,13,14,15



SECURITY RISK PREVENTION STRATEGY:

Initial Risk Impacts:
All risk impacts are assumed to be 100%, which means that the **Threat** is exploiting a **Vulnerability** with probability 100%, then there is total loss of the asset.

As HGA has replaced the modem pool with VPN and added a screened subnet with DMZ, these assets are now being considered for security risk prevention and response strategies. following is the updated list for subset of asset inventory.

Asset Number	Asset Name	Asset Value
A1	Financial Resources	1,000,000
A4	LAN Server	55,000
A7	Router	50,000
A8	Personnel Information	35,000
A16	VPN Server	30,000
A17	DMZ	4,000

With the above assets added to the inventory, the following are the updated threats and vulnerabilities:
Therefore, the following are the updated threat- vulnerabilities pairs:

Subset of Threats:

Threat Number	Threat Name
T1	Payroll Fraud
T3	Interruption of operations
T4	Disclosure or Brokerage of Info
T5	Network- Related attacks
T6	Man-In-The-Middle attack

Subset of Vulnerabilities:

Vulnerability Number	Vulnerability Name
V2	Unauthorized Access
V9	Virus Prevention
V11	Vulnerabilities Related to disclosure or brokerage of information
V12	Vulnerabilities related to Network Related Attacks
V13	Heap buffer overflow vulnerability

Since Vulnerability V9- Virus Prevention is the highest ranked vulnerability, additional controls can be implemented such as implementing advanced encryption methods for communication to servers and on PC hard disks. Implementation of IPS along with routinely updating the signatures can help to mitigate this vulnerability to greater extent.

	T1	T3	T4	T5	T6
V2	15	10	5	10	15
V9	**3**	**5**	**7**	**5**	**3**
V11	10	5	20	20	15
V12	20	10	10	20	15
V13	7	15	15	20	20

Total threat= 295

Residual Asset Security Risks:

Risk of A1= Value of Asset1 (Financial Resources) * Total Threat value
= 1000000*295/100 = 2,950,000> Value of A1
Therefore, Risk of A1= 1,000,000 (total asset loss)

Risk of A4= Value of Asset4 (LAN Server) * Total Threat value/100
= 55,000*295/100 =162,250> Value of A4
Therefore, Risk of A4= 55,000 (total asset loss)

Risk of A7= Value of Asset7 (Router) * Total Threat value/100
= 50000*295/100 = 147,500> Value of A7
Therefore, Risk of A7= 50000 (total asset loss)

Risk of A8= Value of Asset8 (Personnel Information) * Total Threat value/100
= 35000*295/100 = 103,250 > Value of A8

Therefore, Risk of A8= 35000 (total asset loss)

Risk of A16= Value of Asset8 (VPN Server) * Total Threat value/100
= 30000*295/100 = 88,500 > Value of A8
Therefore, Risk of A8= 30000 (total asset loss)

Risk of A8= Value of Asset8 (Personnel Information) * Total Threat value/100
= 4,000*295/100 = 11,200 > Value of A8
Therefore, Risk of A8= 4,000 (total asset loss)

Total Residual Risk= 1,000,000+ 50,000+ 55,000+35,000+30,000+4,000= 1,174,000

- In Risk Management, each asset risk value cannot exceed the risk of the asset. Since the risk exists, based on current controls, the risks calculated above are **Residual Security Risks** of the assets.

Vulnerability Security Risks:

Risk due to Vulnerability 2= Total value of Vulnerability 2* (Value of (A1+A4+A7+A8)) /100
= 55* (1,174,000)/100 = 645,700
Risk due to Vulnerability 9= Total value of Vulnerability 9* (Value of (A1+A4+A7+A8)) /100
= 23* (1,174,000)/100 = 270,020
Risk due to Vulnerability 11= Total value of Vulnerability 11* (Value of (A1+A4+A7+A8)) /100
= 70* (1,174,000)/100 = 821,800
Risk due to Vulnerability 12= Total value of Vulnerability 12* (Value of (A1+A4+A7+A8)) /100
= 75* (1,174,000)/100 = 903,980

Risk due to Vulnerability 13= Total value of Vulnerability 13* (Value of (A1+A4+A7+A8)) /100
= 77* (1,174,000)/100 = 880,500

Ranking of Residual Asset Security Risks:

Rank	Asset Name	Residual Asset Security Risk Value
1	Financial Resources- A1	1,000,000
2	LAN Server-A4	55,000
3	Router-A7	50,000
4	Personnel Information-A8	35,000
5	VPN Server- A16	30,000
6	DMZ- A17	4,000

Ranking of Vulnerability Security Risks:

Rank	Vulnerability Name	Vulnerability Security Risk
1	Vulnerabilities related to Network Related Attacks- V12	903,980
2	Heap Buffer Overflow Vulnerability	880,500
3	Vulnerabilities Related to disclosure or brokerage of information- V11	821,800
4	Unauthorized Access- V2	645,700
5	Virus Prevention- V9	270,020

STEP P2:

	T1	T3	T4	T5	T6
V2	15	10	5	10	15
V9	3	5	7	5	3
V11	10	5	20	20	15
V12	**7**	**5**	**5**	**7**	**7**
V13	7	15	15	20	20

Total Threat= 245

Residual Asset Security Risks:

Risk of A1= Value of Asset1 (Financial Resources) * Total Threat value
= 1000000*245/100 = 2,450,000> Value of A1
Therefore, Risk of A1= 1,000,000 (total asset loss)

Risk of A4= Value of Asset4 (LAN Server) * Total Threat value/100
= 55,000*245/100 =134,750 Value of A4
Therefore, Risk of A4= 55,000 (total asset loss)

Risk of A7= Value of Asset7 (Router) * Total Threat value/100
= 50000*245/100 = 122,500> Value of A7
Therefore, Risk of A7= 50000 (total asset loss)

Risk of A8= Value of Asset8 (Personnel Information) * Total Threat value/100
= 35000*245/100 = 85,750 > Value of A8
Therefore, Risk of A8= 35000 (total asset loss)

Risk of A16= Value of Asset8 (VPN Server) * Total Threat value/100
= 30000*245/100 =73,500 > Value of A8
Therefore, Risk of A8= 30000 (total asset loss)

Risk of A17= Value of Asset8 (Personnel Information) * Total Threat value/100

= 4,000*245/100 = 9,800 > Value of A8
Therefore, Risk of A8= 4,000 (total asset loss)

Total Residual Risk= 1,000,000+ 50,000+ 55,000+35,000+30,000+4,000= 1,174,000

- In Risk Management, each asset risk value cannot exceed the risk of the asset. Since the risk exists, based on current controls, the risks calculated above are **Residual Security Risks** of the assets.

Vulnerability Security Risks:

Risk due to Vulnerability 2= Total value of Vulnerability 2* (Value of (A1+A4+A7+A8)) /100
= 55* (1,174,000)/100 = 645,700
Risk due to Vulnerability 9= Total value of Vulnerability 9* (Value of (A1+A4+A7+A8)) /100
= 23* (1,174,000)/100 = 270,020
Risk due to Vulnerability 11= Total value of Vulnerability 11* (Value of (A1+A4+A7+A8)) /100
= 70* (1,174,000)/100 = 821,800
Risk due to Vulnerability 12= Total value of Vulnerability 12* (Value of (A1+A4+A7+A8)) /100
= 31* (1,174,000)/100 = 363,940
Risk due to Vulnerability 13= Total value of Vulnerability 13* (Value of (A1+A4+A7+A8)) /100
= 22* (1,174,000)/100 = 875,980

Ranking of Residual Asset Security Risks:

Rank	Asset Name	Residual Asset Security Risk Value
1	Financial Resources- A1	1,000,000
2	LAN Server-A4	55,000
3	Router-A7	50,000
4	Personnel Information-A8	35,000
5	VPN Server- A16	30,000
6	DMZ- A17	4,000

Ranking of Vulnerability Security Risks:

Rank	Vulnerability Name	Vulnerability Security Risk
1	Heap Buffer Overflow Vulnerability	875,980
2	Vulnerabilities Related to disclosure or brokerage of information- V11	821,800

3	Unauthorized Access- V2	645,700
4	Vulnerabilities related to Network Related Attacks- V12	363,940
5	Virus Prevention- V9	270,020

STEP P3:

Now after implementing Security Risk Prevention Strategy, Vulnerability V9- Virus Prevention is now the least ranked vulnerability.
Therefore, the new highest ranked vulnerability is V2- Unauthorized Access. Additional hardening controls can be implemented such as implementing VLANS to mitigate “in the clear” conversations. Implementation of Multi Factor Authentication with biometrics/ security device can also help to mitigate this vulnerability and also the other vulnerabilities to greater extent.
Therefore, the following are the updated threat- vulnerabilities pairs:

	T1	T3	T4	T5	T6
V2	15	10	5	10	15
V9	3	5	7	5	3
V11	10	5	20	20	15
V12	7	5	5	7	7
V13	**3**	**5**	**4**	**5**	**5**

Total threat: 210

Residual Asset Security Risks:

Risk of A1= Value of Asset1 (Financial Resources) * Total Threat value
= 1000000*210/100 = 2,100,000> Value of A1
Therefore, Risk of A1= 1,000,000 (total asset loss)

Risk of A4= Value of Asset4 (LAN Server) * Total Threat value/100
= 55,000*210/100 =132,000 Value of A4
Therefore, Risk of A4= 55,000 (total asset loss)

Risk of A7= Value of Asset7 (Router) * Total Threat value/100
= 50000*210/100 = 120,000> Value of A7
Therefore, Risk of A7= 50000 (total asset loss)

Risk of A8= Value of Asset8 (Personnel Information) * Total Threat value/100
= 35000*210/100 = 84,000 > Value of A8
Therefore, Risk of A8= 35000 (total asset loss)

Risk of A16= Value of Asset8 (VPN Server) * Total Threat value/100
= 30000*210/100 = 72,000 > Value of A8

Therefore, Risk of A8= 30000 (total asset loss)

Risk of A8= Value of Asset8 (Personnel Information) * Total Threat value/100
= 4,000*210/100 = 9,600 > Value of A8
Therefore, Risk of A8= 4,000 (total asset loss)

Total Residual Risk= 1,000,000+ 50,000+ 55,000+35,000+30,000+4,000= 1,174,000

- In Risk Management, each asset risk value cannot exceed the risk of the asset. Since the risk exists, based on current controls, the risks calculated above are **Residual Security Risks** of the assets.

Vulnerability Security Risks:

Risk due to Vulnerability 2= Total value of Vulnerability 2* (Value of (A1+A4+A7+A8)) /100
= 55* (1,174,000)/100 = 645,700
Risk due to Vulnerability 9= Total value of Vulnerability 9* (Value of (A1+A4+A7+A8)) /100
= 23* (1,174,000)/100 = 270,020
Risk due to Vulnerability 11= Total value of Vulnerability 11* (Value of (A1+A4+A7+A8)) /100
= 70* (1,174,000)/100 = 821,800
Risk due to Vulnerability 12= Total value of Vulnerability 12* (Value of (A1+A4+A7+A8)) /100
= 31* (1,174,000)/100 = 363,940
Risk due to Vulnerability 13= Total value of Vulnerability 13* (Value of (A1+A4+A7+A8)) /100
= 22* (1,174,000)/100 = 258,280

Ranking of Residual Asset Security Risks:

Rank	Asset Name	Residual Asset Security Risk Value
1	Financial Resources- A1	1,000,000
2	LAN Server-A4	55,000
3	Router-A7	50,000
4	Personnel Information-A8	35,000
5	VPN Server- A16	30,000
6	DMZ- A17	4,000

Ranking of Vulnerability Security Risks:

Rank	Vulnerability Name	Vulnerability Security Risk

1	Vulnerabilities Related to disclosure or brokerage of information- V11	821,800
2	Unauthorized Access- V2	645,700
3	Vulnerabilities related to Network Related Attacks- V12	363,940
4	Virus Prevention- V9	270,020
5	Heap Buffer Overflow Vulnerability- V13	258,280

Comparing the current various controls discussed to common criteria:
Along with the current controls in place for HGA and the new controls recommended by CISO, additional controls of implementing VPN and DMZ have strengthened the security posture of HGA. Although HGA has effectively implemented few of the controls relevant to the controls listed in Common Criteria, it doesn't look into Environment Protection, Personnel Security and Supply Chain Risk Management Controls.

SECURITY RESPONSE STRATEGY

STEP R1:
Threat- Vulnerability Pairs from step P3:

	T1	T3	T4	T5	T6
V2	15	10	5	10	15
V9	3	5	7	5	3
V11	10	5	20	20	15
V12	7	5	5	7	7
V13	3	5	4	5	5

Risk Impact Matrix:

	T1*V2	T1*V9	T1*V11	T1*V12	T1*V13	T3*V2	T3*V9	T3*V11	T3*V12	T3*V13	T4*V2	T4*V9	T4XV11	T4XV12
A1	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A4	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A7	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A8	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A16	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A17	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

	T4*V13	T5*V2	T5*V9	T5*V11	T5*V12	T5*V13	T6*V2	T6*V9	T6*V11	T6*V12	T6*V13
A1	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A4	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A7	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A8	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

A16	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A17	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

<u>Residual Asset Security Risks:</u>

Residual Risk of Asset1:
1,000,000*
((15*40)+(10*40)+(5*40)+(10*40)+(15*40)+(3*40)+(5*40)+(7*40)+(5*40)+(3*40)+(10*40)+(5*40)+(20*40)+(20*40)+(15*40)+(7*40)+(5*40)+(5*40)+(7*40)+(7*40)+(3*40)+(5*40)+(4*40)+(5*40) +(5*40))
2,200+1200+920+3000+2200+880
=1,040,000

Residual Risk of Asset4:
55,000*
((15*40)+(10*40)+(5*40)+(10*40)+(15*40)+(3*40)+(5*40)+(7*40)+(5*40)+(3*40)+(10*40)+(5*40)+(20*40)+(20*40)+(15*40)+(7*40)+(5*40)+(5*40)+(7*40)+(7*40)+(3*40)+(5*40)+(4*40)+(5*40) +(5*40))
= 39,768< 57,200

Residual Risk of Asset 7:
50,0000*
((15*40)+(10*40)+(5*40)+(10*40)+(15*40)+(3*40)+(5*40)+(7*40)+(5*40)+(3*40)+(10*40)+(5*40)+(20*40)+(20*40)+(15*40)+(7*40)+(5*40)+(5*40)+(7*40)+(7*40)+(3*40)+(5*40)+(4*40)+(5*40) +(5*40))
=52,000

Residual Risk of Asset 8:
35,000*
((15*40)+(10*40)+(5*40)+(10*40)+(15*40)+(3*40)+(5*40)+(7*40)+(5*40)+(3*40)+(10*40)+(5*40)+(20*40)+(20*40)+(15*40)+(7*40)+(5*40)+(5*40)+(7*40)+(7*40)+(3*40)+(5*40)+(4*40)+(5*40) +(5*40))
= 36,400

Residual Risk of Asset 16:
30,000*
((15*40)+(10*40)+(5*40)+(10*40)+(15*40)+(3*40)+(5*40)+(7*40)+(5*40)+(3*40)+(10*40)+(5*40)+(20*40)+(20*40)+(15*40)+(7*40)+(5*40)+(5*40)+(5*40)+(7*40)+(3*40)+(5*40)+(4*40)+(5*40) +(5*40))
= 31,200

Residual Risk of Asset 17:
4,000*
((15*40)+(10*40)+(5*40)+(10*40)+(15*40)+(3*40)+(5*40)+(7*40)+(5*40)+(3*40)+(10*40)+(5*40)+(20*40)+(20*40)+(15*40)+(7*40)+(5*40)+(5*40)+(7*40)+(7*40)+(3*40)+(5*40)+(4*40)+(5*40) +(5*40))

= 4,160

Security Vulnerability Risk:

Vulnerability Risk V2:

1000000*(15*40 +10*60 +5*40 +15*40 +10*40) + 55,000*(15*40 +10*40 +5*40 +15*40 +10*40) + 50,000*(15*40 +10*40 +5*40 +15*40 +10*40)+ 35,000*(15*40 +10*40 +5*40 +15*40 +10*40) + 30,000*(15*40 +10*40 +5*40 +15*40 +10*40)+4,000*(15*40 +10*40 +5*40 +15*40 +10*40)
= 330,000+12,100+11,000+7,700+6,600+880= $368,280

Vulnerability Risk V9:

1000000*(3*40 +5*40 +7*40 +5*40 +3*40) + 55,000*(3*40 +5*40 +7*40 +5*40 +3*40) + 50,000*(3*40 +5*40 +7*40 +5*40 +3*40) + 35,000*(3*40 +5*40 +7*40 +5*40 +3*40) + 30,000*(3*40 +5*40 +7*40 +5*40 +3*40) +4,000*(3*40 +5*40 +7*40 +5*40 +3*40)
=92,000+5,060+4,600+3,220+2760+368
=108,008

Vulnerability Risk V11:

1000000*(10*40 +5*40 +20*40 +20*40 +15*40) + 55,000*(10*40 +5*40 +20*40 +20*40 +15*40) + 50,000*(10*40 +5*40 +20*40 +20*40 +15*40) + 35,000*(10*40 +5*40 +20*40 +20*40 +15*40) + 30,000*(10*40 +5*40 +20*40 +20*40 +15*40) +4,000*(10*40 +5*40 +20*40 +20*40 +15*40)
=280,000+15400+14000+9800+8400+1120
=328,720

Vulnerability Risk V12:

1000000*(7*40 +5*40 +5*40 +7*40 +7*40) + 55,000*(7*40 +5*40 +5*40 +7*40 +7*40) + 50,000*(7*40 +5*40 +5*40 +7*40 +7*40) + 35,000*(7*40 +5*40 +5*40 +7*40 +7*40) + 30,000*(7*40 +5*40 +5*40 +7*40 +7*40) +4,000*(7*40 +5*40 +5*40 +7*40 +7*40) =
=124,000+6820+6200+4340+3720+496
=145,576

Vulnerability Risk V12:

1000000*(3*40 +5*40+4*40+5*40+5*40) + 55,000*(3*60 +5*60 +4*60 +5*60 +5*60) + 50,000*(3*60 +5*60 +4*60 +5*60 +5*60) + 35,000*(3*60 +5*60 +4*60 +5*60 +5*60) + 30,000*(3*60 +5*60 +4*60 +5*60 +5*60) +4,000*(3*60 +5*60 +4*60 +5*60 +5*60)
=103,312

Ranking of Residual Asset Security Risks:

Rank	Asset Name
1	Financial Resources- A1
2	LAN Server-A4
3	Router-A7
4	Personnel Information-A8
5	VPN Server- A16
6	DMZ- A17

Ranking of Vulnerability Security Risks:

Rank	Vulnerability Name
1	Unauthorized Access- V2
2	Vulnerabilities Related to disclosure or brokerage of information- V11
3	Vulnerabilities related to Network Related Attacks- V12
4	Virus Prevention- V9
5	Heap Buffer Overflow Vulnerability- V13

STEP R2:

Since Residual Asset A7- Router is the highest ranked Residual Asset Risk, additional controls can be implemented such as non-essential services and implementing periodic review of the access controls. Implementation of redundant servers can help to mitigate this vulnerability to greater extent.

Therefore, the following are the updated Risk- Impact Probabilities:

Threat- Vulnerability Pairs from step P3:

	T1	T3	T4	T5	T6
V2	7	3	2	5	7
V9	3	5	7	5	3
V11	5	5	7	7	7
V12	7	5	5	7	7
V13	3	5	4	5	5

Risk Impact Matrix:

	T1*V2	T1*V9	T1*V11	T1*V12	T1*V13	T3*V2	T3*V9	T3*V11	T3*V12	T3*V13	T4*V2	T4*V9	T4XV11	T4XV12
A1	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A4	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A7	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A8	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A16	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A17	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

	T4*V13	T5*V2	T5*V9	T5*V11	T5*V12	T5*V13	T6*V2	T6*V9	T6*V11	T6*V12	T6*V13
A1	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A4	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A7	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A8	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

A16	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A17	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

Residual Asset Security Risks:

Residual Risk of Asset1:
=1000000*
(7*5+3*5+5*5+7*5+3*5+3*5+5*5+5*5+5*5+5*5+2*5+7*5+7*5+5*5+4*5+5*5+5*5+7*5+7*5+5*5+7*5+3*5+7*5+7*5+5*5)=
=10000*(125+ 115+125+290)= 65,500
Therefore, Risk of A1 gives partial asset loss

Residual Risk of Asset4:
=55,000*
(7*40+3*40+5*40+7*40+3*40+3*40+5*40+5*40+5*40+5*40+2*40+7*40+7*40+5*40+4*40+5*40+5*40+7*40+7*40+5*40+7*40+3*40+7*40+7*40+5*40)
=55,000*(1000+1280+1600+1360)
=28,820
Therefore, Risk of A4 gives partial asset loss

Residual Risk of Asset 7:
=50,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)
=26,200
Therefore, Risk of A7 gives partial asset loss

Residual Risk of Asset 8:
=35,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 60,750
Therefore, Risk of A8 gives partial asset loss
18,340

Residual Risk of Asset 16:
=30,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 15,720
Therefore, Risk of A16 gives partial asset loss

Residual Risk of Asset 17:

=4,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 2,096
Therefore, Risk of A17 gives partial asset loss

<u>Security Vulnerability Risk:</u>

Vulnerability Risk V2:

1000000*(7*5+3*5+2*5+5*5+7*5) + 55,000*(7*40+3*40+2*40+5*40+7*40) +
50,000*(7*40+3*40+2*40+5*40+7*40)+ 35,000*(7*40+3*40+2*40+5*40+7*40) +
30,000*(7*40+3*40+2*40+5*40+7*40)+4,000*(7*40+3*40+2*40+5*40+7*40)
=12000+5280+4800+3360+2880+384
=28,704

Vulnerability Risk V9:

1000000*(3*5+5*5+7*5+5*5+3*5) + 55,000*(3*40+5*40+7*40+5*40+3*40) +
50,000*(3*40+5*40+7*40+5*40+3*40)+ 35,000*(3*40+5*40+7*40+5*40+3*40) +
30,000*(3*40+5*40+7*40+5*40+3*40)+4,000*(3*40+5*40+7*40+5*40+3*40
=11,500+ 5060+4600+3220+2760+368
=27,508

Vulnerability Risk V11:

1000000*(5*5+5*5+7*5+7*5+7*5) + 55,000*(5*40+5*40+7*40+7*40+7*40) +
50,000*(5*40+5*40+7*40+7*40+7*40)+ 35,000*(5*40+5*40+7*40+7*40+7*40) +
30,000*(5*40+5*40+7*40+7*40+7*40)+4,000*(5*40+5*40+7*40+7*40+7*40)
=15500+6820+6200+4340+3720+496
=37076

Vulnerability Risk V12:

1000000*(7*5+5*5+5*5+7*5+7*5) + 55,000*(7*40+5*40+5*40+7*40+7*40) +
50,000*(7*40+5*40+5*40+7*40+7*40)+ 35,000*(7*40+5*40+5*40+7*40+7*40) +
30,000*(7*40+5*40+5*40+7*40+7*40)+4,000*(7*40+5*40+5*40+7*40+7*40)
=15,500+6820+6200+4340+3720+496
=37,076

Vulnerability Risk V13:

1000000*(3*5+5*5+4*5+5*5+5*5) + 55,000*(3*40+5*40+4*40+5*40+5*40) +
50,000*(3*40+5*40+4*40+5*40+5*40)+ 35,000*(3*40+5*40+4*40+5*40+5*40) +
30,000*(3*40+5*40+4*40+5*40+5*40)+4,000*(3*40+5*40+4*40+5*40+5*40)
=11000+4840+4400+3080+2640+352
=26,312

Ranking of Residual Asset Security Risks:

Rank	Asset Name
1	Financial Resources- A1
2	LAN Server-A4
3	Router-A7
4	Personnel Information-A8
5	VPN Server- A16
6	DMZ- A17

Ranking of Vulnerability Security Risks:

Rank	Vulnerability Name
1	Vulnerabilities Related to disclosure or brokerage of information- V11
2	Vulnerabilities related to Network Related Attacks- V12
3	Unauthorized Access- V2
4	Virus Prevention- V9
5	Heap Buffer Overflow Vulnerability- V13

<u>**STEP R3:**</u>

Now after implementing **Security Risk Response (Resilience) Strategy**, Resiudual Asset- A8 Router is now the least ranked Residual Asset Risk.

Therefore, the new highest ranked Residual Asset Risk is A1- Financial resources. Additional hardening controls can be implemented such as restricting attempts for passwords and restriction of services that impact operational effectiveness.

	T1	T3	T4	T5	T6
V2	7	3	2	5	7
V9	3	5	7	5	3
V11	5	5	7	7	7
V12	7	5	5	7	7
V13	3	5	4	5	5

Risk Impact Matrix:

	T1*V2	T1*V9	T1*V11	T1*V12	T1*V13	T3*V2	T3*V9	T3*V11	T3*V12	T3*V13	T4*V2	T4*V9	T4XV11	T4XV12
A1	2%	2%	2%	2%	2%	1%	1%	1%	1%	1%	1%	1%	2%	2%
A4	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A7	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A8	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A16	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A17	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

	T4*V13	T5*V2	T5*V9	T5*V11	T5*V12	T5*V13	T6*V2	T6*V9	T6*V11	T6*V12	T6*V13

A1	2%	2%	2%	2%	2%	1%	1%	1%	1%	1%	1%
A4	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A7	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A8	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A16	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%
A17	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%	40%

Residual Asset Security Risks:

Residual Risk of Asset1:
=1000000*
(7*2+3*2+5*2+7*2+3*2+3+5+5+5+5+2+7*2+7*2+5*2+4*2+5*2+5*2+7*2+7+5+7+3+7+7+5)
= 1000000*(50+25+80+41)
=19,600

Therefore, Risk of A1 gives partial asset loss

Residual Risk of Asset4:
=55,000*
(7*40+3*40+5*40+7*40+3*40+3*40+5*40+5*40+5*40+5*40+2*40+7*40+7*40+5*40+4*40+5*40+5*40+7*40+7*40+5*40+7*40+3*40+7*40+7*40+5*40)
=55,000*(1000+1280+1600+1360)
=28,820
Therefore, Risk of A4 gives partial asset loss

Residual Risk of Asset 7:
=50,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)
=26,200
Therefore, Risk of A7 gives partial asset loss

Residual Risk of Asset 8:
=35,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 60,750
Therefore, Risk of A8 gives partial asset loss
18,340

Residual Risk of Asset 16:
=30,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*6

0+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 15,720
Therefore, Risk of A16 gives partial asset loss

Residual Risk of Asset 17:
=4,000*
(15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 2,096
Therefore, Risk of A17 gives partial asset loss

<u>Security Vulnerability Risk:</u>

<u>Security Vulnerability Risk:</u>

Vulnerability Risk V2:
1000000*(7*2+3*2+2*2+5*2+7*2) + 55,000*(7*40+3*40+2*40+5*40+7*40) +
50,000*(7*40+3*40+2*40+5*40+7*40)+ 35,000*(7*40+3*40+2*40+5*40+7*40) +
30,000*(7*40+3*40+2*40+5*40+7*40)+4,000*(7*40+3*40+2*40+5*40+7*40)
=4800+5280+4800+3360+2880+384
=21,504

Vulnerability Risk V9:
1000000*(3+5+7+5+3) + 55,000*(3*40+5*40+7*40+5*40+3*40) +
50,000*(3*40+5*40+7*40+5*40+3*40)+ 35,000*(3*40+5*40+7*40+5*40+3*40) +
30,000*(3*40+5*40+7*40+5*40+3*40)+4,000*(3*40+5*40+7*40+5*40+3*40
=2300+ 5060+4600+3220+2760+368
=18308

Vulnerability Risk V11:
1000000*(5+5+7*2+7*2+7*2) + 55,000*(5*40+5*40+7*40+7*40+7*40) +
50,000*(5*40+5*40+7*40+7*40+7*40)+ 35,000*(5*40+5*40+7*40+7*40+7*40) +
30,000*(5*40+5*40+7*40+7*40+7*40)+4,000*(5*40+5*40+7*40+7*40+7*40)
=5200+6820+6200+4340+3720+496
=26,776

Vulnerability Risk V12:
1000000*(7*2+5*2+5*2+7*2+7) + 55,000*(7*40+5*40+5*40+7*40+7*40) +
50,000*(7*40+5*40+5*40+7*40+7*40)+ 35,000*(7*40+5*40+5*40+7*40+7*40) +
30,000*(7*40+5*40+5*40+7*40+7*40)+4,000*(7*40+5*40+5*40+7*40+7*40)
=5,500+6820+6200+4340+3720+496
=27,076

Vulnerability Risk V13:
1000000*(3+5+4+5+5) + 55,000*(3*40+5*40+4*40+5*40+5*40) +
50,000*(3*40+5*40+4*40+5*40+5*40)+ 35,000*(3*40+5*40+4*40+5*40+5*40) +
30,000*(3*40+5*40+4*40+5*40+5*40)+4,000*(3*40+5*40+4*40+5*40+5*40)
=2200+4840+4400+3080+2640+352
=17512

Ranking of Residual Asset Security Risks:

Rank	**Asset Name**	Residual Asset Security Risk
1	LAN Server- A4	L
2	Router- A7	L
3	Personnel Information- A8	L
4	Financial Resources-A1	L

Ranking of Residual Asset Security Risks:

Rank	Asset Name
1	LAN Server-A4
2	Router-A7
3	Personnel Information-A8
4	VPN Server- A16
5	DMZ- A17
6	Financial Resources- A1

Ranking of Vulnerability Security Risks:

Rank	Vulnerability Name
1	Vulnerabilities related to Network Related Attacks- V12
2	Vulnerabilities Related to disclosure or brokerage of information- V11
3	Unauthorized Access- V2
4	Virus Prevention- V9
5	Heap Buffer Overflow Vulnerability- V13

Comparing the current various response controls discussed to common criteria:
Along with the current controls in place for HGA and the new controls recommended by CISO, additional controls of implementing VPN and DMZ have strengthened the security posture of HGA. Although HGA has effectively implemented few of the response controls by using redundant servers and stronger password policy, relevant to the controls listed in Common Criteria, it needs to look more into strengthening of Audit Accountability, Configuration Management and Supply Chain Risk Management Controls.

MIXED STRATEGY:

Based on various additional hardening controls, the probability for failure has been reduced to a greater extent. In this Mixed Strategy implementation, the following new controls are implemented to further reduce the probabilities.

Managerial	Operational	Technical
Authorize Processing (Certification and Accreditation)	Documentation of using Removable Media	Strong I&A Systems
LAN Server Access specific policy	Redundant Server	Installation of Unified Threat Management services
	Incident Response Capability	Audit Trails
	Periodic maintenance and patch management	
	Data Integrity	

	T1	T3	T4	T5	T6
V2	2	0	0	1	2
V9	0	1	2	1	0
V11	1	1	2	2	2
V12	2	1	1	2	2
V13	0	1	0	1	1

Risk Impact Matrix:

	T1*V2	T1*V9	T1*V11	T1*V12	T1*V13	T3*V2	T3*V9	T3*V11	T3*V12	T3*V13	T4*V2	T4*V9	T4XV11	T4XV12
A1	2%	2%	2%	2%	2%	1%	1%	1%	1%	1%	1%	1%	2%	2%
A4	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%
A8	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A16	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A17	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%

	T4*V13	T5*V2	T5*V9	T5*V11	T5*V12	T5*V13	T6*V2	T6*V9	T6*V11	T6*V12	T6*V13
A1	2%	2%	2%	2%	2%	1%	1%	1%	1%	1%	1%
A4	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A7	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A8	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A16	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A17	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%

Residual Asset Security Risks:

Residual Risk of Asset1:

=1000000* (1*2+2+2*2+1+1+1+1+2*2+2*2+2+2+2+2*2+2*2+1+2+2+2+1)

= 1000000*(42)

=420

Therefore, Risk of A1 gives partial asset loss

Residual Risk of Asset4:

=55,000* (2*10+1*10+2*10+1*10+1*10+1*10+1*10+2*10+2*10+1*10+1*10+1*10+2*10+2*10+2*10+1*10+2*10+2*10+1*10)

=55,000*(90+130+60)

=1540

Therefore, Risk of A4 gives partial asset loss

Residual Risk of Asset 7:

=50,000* (15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)

=1400

Therefore, Risk of A7 gives partial asset loss

Residual Risk of Asset 8:

=35,000* (15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 980

Therefore, Risk of A8 gives partial asset loss

Residual Risk of Asset 16:

=30,000* (15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 840

Therefore, Risk of A16 gives partial asset loss

Residual Risk of Asset 17:

=4,000* (15*10+3*10+10*10+20*10+3*10+10*60+5*60+5*60+10*60+5*60+5*60+7*60+20*60+10*60+4*60+10*60+5*60+20*60+20*60+5*60+15*60+3*60+15*60+15*60+5*60)= 112

Therefore, Risk of A17 gives partial asset loss

Security Vulnerability Risk:

Vulnerability Risk V2:

1000000*(2*2+1+2*2) + 55,000*(2*10+10+2*10) + 50,000*(2*10+10+2*10)+
35,000*(2*10+10+2*10) + 30,000*(2*10+10+2*10)+4,000*(2*10+10+2*10)
=900+ 275+250+175+150+20
=1770

Vulnerability Risk V9:

1000000*(1*1+2*1+2*1) + 55,000*(1*10+2*10+1*10)+ 50,000*(1*10+2*10+1*10)+
35,000*(1*10+2*10+1*10) + 30,000*(1*10+2*10+1*10)+4,000*(1*10+2*10+1*10)
=500+ 220+200+140+120+16
=1196

Vulnerability Risk V11:

1000000*(2+1+2*2+2*2+1*2) + 55,000*(1*10+1*10+2*10+2*10+2*10) +
50,000*(1*10+1*10+2*10+2*10+2*10)+ 35,000*(1*10+1*10+2*10+2*10+2*10) +
30,000*(1*10+1*10+2*10+2*10+2*10)+4,000*(1*10+1*10+2*10+2*10+2*10)
=1300+440+400+280+240+32
=2692

Vulnerability Risk V12:

1000000*(2*2+1*1+1*2+2*2+2) + 55,000*(2*10+1*10+1*10+2*10+2*10) +
50,000*(2*10+1*10+1*10+2*10+2*10)+ 35,000*(2*10+1*10+1*10+2*10+2*10) +
30,000*(2*10+1*10+1*10+2*10+2*10)+4,000*(2*10+1*10+1*10+2*10+2*10)
=1300+440+400+280+240+32
=2692

Vulnerability Risk V13:

1000000*(1+1+1) + 55,000*(1*10+1*10+1*10) + 50,000*(1*10+1*10+1*10)+
35,000*(1*10+1*10+1*10) + 30,000*(1*10+1*10+1*10)+4,000*(1*10+1*10+1*10)
=300+165+150+105+90+12
=822

Ranking of Residual Asset Security Risks:

Rank	Asset Name
1	LAN Server-A4
2	Router-A7
3	Personnel Information-A8
4	VPN Server- A16
5	Financial Resources- A1
6	DMZ- A17

Ranking of Vulnerability Security Risks:

Rank	Vulnerability Name
1	Vulnerabilities related to Network Related Attacks- V12
2	Vulnerabilities Related to disclosure or brokerage of information- V11
3	Unauthorized Access- V2
4	Virus Prevention- V9
5	Heap Buffer Overflow Vulnerability- V13

COST BENEFIT ANALYSIS:

The security risk assessment for Hypothetical Government Agency (HGA) provides a detailed quantitative security risk analysis for HGA's critical assets. This risk assessment listed out various threats and vulnerabilities that could potentially impact the critical assets of HGA (as listed in HGA case study). It then considered a smaller subset of critical assets, threat vulnerability pairs and calculated their respective Residual Asset Security Risks and Vulnerability Security Risks for the following 3 scenarios:

a) current security controls b) new controls provided by CISO and c) Management-Operational-Technical Controls.

HGA's risk management recommendations were satisfactory in order to carry every day required operations for the organization. But its security program did not implement necessary controls to prevent its valuable information assets from potential cyber-attacks. Based on the risk assessment evaluation and detailed study conducted by HGA, it determined that there were various potential vulnerabilities whose mitigation required higher financial costs. Therefore, such vulnerabilities were being accepted by HGA without any mitigations. Also, few of the mitigations recommended were contradicting with each other resulting in unsuccessful implementation of such mitigations and leaving a greater attack surface.

HGA has efficiently documented various security controls for assessing the risks to their asset inventory but failed to adhere to their documentation and policies for periodic review. When the effectiveness of security risks was reviewed by HGA, few of the additional controls recommended by CISO were successfully implemented. Additionally, various recommendations were provided by CISO to mitigate certain threats to their critical assets, but these recommendations incurred huge financial input, and thus such risks were being accepted by the management. HGA has also appropriately classified the privileges and implemented least privilege policy and accountability. But the physical security and criminal record check were not considered within the scope of this analysis. Based on new controls recommended by CISO, HGA implemented controls for protecting mobile and portable systems and implemented media controls. While conducting the security risk assessment, HGA did a great job in identifying the most critical assets but scoped out the physical security and interconnected systems. HGA's contingency plan and disaster recovery plans were improvised based on the recommendation by CISO. And the controls were implemented for accessing system software & hardware, for reducing various vulnerabilities and providing adequate training to the employees.

Nevertheless, HGA did a great job in addressing the threat posed by the implementation of modem and effectively improvised the access controls and information access via the VPN and DMZ server. The systems controls did not provide access to the public. Moreover, the access to critical files were effectively logged, monitored and efficiently restricted from inappropriate access. HGA had also implemented various policies to address Managerial controls from M-O-T model but were unsuccessful in implementing/ following the policies. During the Risk Assessment, HGA decided to implement various Operational Controls such as improved security training, providing backups for 5% of their PC's, which were satisfactory to reduce the risk impact and improve resilience. The Technical Controls implemented by HGA were successful in mitigating few existing vulnerabilities, but it still did not address weak Server Access Controls and I&A System which were critical to information asset inventory of HGA.

During the Risk Prevention Strategy, the modem pool was replaced with a VPN server and a screened subnet with DMZ was added. As a result, the asset inventory of HGA increased and threat-vulnerability pairs impacting the newly added assets were considered under the scope for risk assessment.
After reducing the overall security residual asset risk and vulnerability security risk by implementing Security Risk Prevention Strategy, the threat vulnerability pairs probabilities were reduced to a greater extent. Now Security Risk Response Strategy was executed on this updated threat vulnerability pair probabilities. Therefore, under this strategy additional hardening controls were implemented on the highest ranked residual asset risk. Also, the resilience of critical assets was being considered in this strategy in order to measure the effectiveness of the security controls which provided the resilience for the critical assets.

In conclusion, Risk Prevention and Risk Response are great strategies order to assess the impact of risk and develop mitigations/ resilience. While the Risk Prevention Strategy considers the scenario before an attack occurs and assesses the impact of the risk on the asset's values. The Risk Response Strategy helps to identify the resilience strength and how it reduces the destruction of asset value. Moreover, under the Mixed Strategy, the threat vulnerability pairs, and resilience probabilities were updated after implementing appropriate controls from Security Risk Prevention Strategy and Security Risk Response Strategy and any new controls if deemed appropriate. The Residual Asset Security Risks and Vulnerability Security Risks were again calculated. In my opinion, the Mixed strategy provides an efficient method to conduct the assessment considering the characteristics of both Risk Prevention and Risk Response strategies and thus giving an overall view for the Security Risk Assessment of HGA.

The Budget for proposed controls:

Controls Mitigating	Risk Prevention	Risk Response	Risk Strategy
Payroll Fraud	$50,000	$70,000	$120,000
Interruption of operations	$30,000	$50,000	$60,000
Disclosure or Brokerage of Info	$40,000	$55,000	$70,000
Network- Related attacks	$60,000	$90,000	$100,000
VPN	$30,000	$30,000	$70,000
DMZ	$10,000	$10,000	$50,000
Total	$220,000	$305,000	$470,000

Residual Risk= Risk with current controls- Risk with new controls
1,174,000 – 4,972 = 1,169,028

Proposed Security Budget Cost for 3 budgets:

- Cost benefit ratio analysis for risk prevention budget
  - Proposed Security Risk Budget cost/ expected security risk benefit
    = 220,000 / 1,169,028 = 0.19

- Cost benefit ratio analysis for risk response budget
  - Proposed Security Risk Budget cost/ expected security risk benefit
    = 305,000 / 1,169,028 = 0.26

- Cost benefit ratio analysis for risk response budget
  - Proposed Security Risk Budget cost/ expected security risk benefit
    = 470,000 / 1,169,028 =0.4

PART B- SECURITY RISK MANAGEMENT IMPLEMENTATION PLAN

List company critical assets, missing controls, vulnerabilities, potential threats, and security risks for:

Access Control Security Risk Management Implementation Controls and Policies

a) Identification Credentials
b) Personal Authentication
c) Authorization
d) Logical Access Control Methods
e) Physical Access Control Methods
f) Biometric Systems

The following are the list of critical assets present in Symetrica:

ASSET	**ASSET NAME**	Asset Value
A1	Backbone Switch	$15,000
A2	Cable Modem	$35,000
A3	Switches (X4)	$20,000
A4	W Access Points (X5)	$25,000
A5	**MISys** (maintains inventory)	$75,000
A6	**Symetrica US Server-03**	$100,000
A7	**Arena** (all data and processes tied to the product)	$50,000
A11	QNAP NAS	$65,000
A12	UPS	$30,000
A13	**Firewall Sophos-XG-125**	$55,000
A14	AWS Fleet Servers and services	$30,000
A15	**Gitlab** services	$15,000
A16	Jenkins/Builder	$45,000
A17	PC's	$85,000
A18	Printers	$20,000
A19	Phabricator	$60,000
A20	Internal Correspondence	Intangible
A21	Personnel Information	Intangible
A22	Contracting and Procurement Documents	Intangible
A23	Reputation (Intangible)	Intangible
A24	Employee Confidence (Intangible)	Intangible

List of missing controls:

Missing Controls
Identification Controls
Biometric Feature
Authentication
Fingerprint Verification
Hand Geometry

Cryptographic Hardware Token
Authorization
Security Tokens
Logical Access Control Methods:
Physical Security for SIPRNeT ports
PKI Compliance Requirements
Port Authentication using 802.1X
PKI Certificate
Physical Access Control Methods
Memory Cards
Physical Tokens
Biometric Systems:
Fingerprint Reader
Hand Geometry Reader
Iris Scanner

Vulnerability Name
Vulnerabilities Related to authentication logic and Insecure session handling
vulnerabilities related to internal corporate attacks and disclosure or brokerage of information
Unauthorized Access and missing lock out process
Vulnerabilities related to Unauthorized Access, Vulnerabilities Related to Interruption of Operations

Threat Name
Operating System and escalated priviliges Attacks
Manual exploitation of logical flaws and Heap Buffer Overflow Attacks
Retrieval of unauthorized data and Man-In-The-Middle attack
Retrieval of unauthenticated data and overriding authenticated sessions- session hijacking
Brute force attacks, user enumeration and denial of service attacks

Risks
Might cause interruption of operations due to authenticating non trusted access
It might result in operating system attacks and unavailability of services
It might result in network related attacks, improper functioning of infrastructure & non-compliance
Unauthorized Access might result in damage and loss of physical assets

Network Infrastructure Security Risk Management Implementation Controls and Policies

a) Enclave Protection
b) Firewalls Risk Management
c) Routers Risk Management

The following are the list of critical assets present in Symetrica:

ASSET	**ASSET NAME**	Asset Value
A1	Backbone Switch	$15,000
A2	Cable Modem	$35,000
A3	Switches (X4)	$20,000
A4	W Access Points (X5)	$25,000
A5	**MISys** (maintains inventory)	$75,000
A6	**Symetrica US Server-03**	$100,000
A7	**Arena** (all data and processes tied to the product)	$50,000
A11	QNAP NAS	$65,000
A12	UPS	$30,000
A13	**Firewall Sophos-XG-125**	$55,000
A14	AWS Fleet Servers and services	$30,000
A15	**Gitlab** services	$15,000
A16	Jenkins/Builder	$45,000
A17	PC's	$85,000
A18	Printers	$20,000
A19	Phabricator	$60,000
A20	Internal Correspondence	Intangible
A21	Personnel Information	Intangible
A22	Contracting and Procurement Documents	Intangible
A23	Reputation (Intangible)	Intangible
A24	Employee Confidence (Intangible)	Intangible

List of missing controls:

Missing Controls
Enclave Protection
Intrusion Detection System
Demilitarized Zone
Approved Gateways
Network Test Access Ports
Wireless IDS
Firewalls Risk Management
Packet filter
Bastion Host
Stateful Inspection
Application Proxy Gateway
Hybrid Technology Firewalls
Proxy Servers

Vulnerability Name
Vulnerabilities Related to access control, vulnerabilities related to IP addresses, ports and services disclosure.
vulnerabilities related to malicious traffic, website breaches and data exfiltration
Rogue WIFI Access Points (WAPS), Vulnerabilities related to non-encrypted 802.11 traffic
Private IP Address disclosure, malicious software related attacks

Threat Name
network reconnaissance and IP spoofing, escalated privileges Attacks
DDOS attack, cross site scripting and SQL injection attacks
Outbound email attacks, Threats related to downloads to insecure devices, uploads to cloud storage and unsecured behavior in cloud
Retrieval of unauthorized data and Man-In-The-Middle attack
Network Layer attacks, social engineering attacks, retrieval of unauthenticated data, website cookie exploitation and overriding authenticated sessions- session hijacking

Risks

Deteriorating the throughput of network's links, possibility of DOS attacks and unavailability of services
Loss of Personally Identified Information, Breaches on FTP and HTTPS sites, attacks related to accepting uploaded data.
Masquerading as an authorized user, data modification and creation of backdoors to internal network due to rogue APs.
Data Breaches, unauthorized access might result in damage and installation of malware on systems.

Network Infrastructure Management Security Risk Management Implementation Controls and Policies

a. Ports, Protocols, and Services (PPS) Risk Management
b. Device Risk Management
c. Device Monitoring, Network Management Risk Management
d. Network Authentication, Authorization, and Accounting Risk Management
e. Network Intrusion Detection Risk Management
f. Switches and VLANs Risk Management
g. Virtual Private Network Risk Management

The following are the list of critical assets present in Symetrica:

ASSET	**ASSET NAME**	Asset Value
A1	Backbone Switch	$15,000
A2	Cable Modem	$35,000
A3	Switches (X4)	$20,000
A4	W Access Points (X5)	$25,000
A5	**MISys** (maintains inventory)	$75,000
A6	**Symetrica US Server-03**	$100,000
A7	**Arena** (all data and processes tied to the product)	$50,000
A11	QNAP NAS	$65,000
A12	UPS	$30,000
A13	**Firewall Sophos-XG-125**	$55,000
A14	AWS Fleet Servers and services	$30,000
A15	**Gitlab** services	$15,000
A16	Jenkins/Builder	$45,000
A17	PC's	$85,000
A18	Printers	$20,000
A19	Phabricator	$60,000
A20	Internal Correspondence	Intangible
A21	Personnel Information	Intangible
A22	Contracting and Procurement Documents	Intangible

A23	Reputation (Intangible)	Intangible
A24	Employee Confidence (Intangible)	Intangible

List of missing controls:

Missing Controls
Ports, Protocols, and Services (PPS) Risk Management
Restricting ICMPv4 message
Unicast Reverse Path Forwarding
Protection against SYN Flood Attack
Device Risk Management
Out-of-band device management
In-band device management
Network Authentication, Authorization, and Accounting Risk Management
Accounting
Auditing
Router Password Protection
Network Intrusion Detection Risk Management
Local Area NIDS
Switches and VLANs Risk Management
VLAN Port Security
VLAN 802.1x and Management Policy Server
Virtual Private Network Risk Management
Host to host

Vulnerability Name
Improper memory resource management, missing input validation, improper error handling
Improper filtration of serialized input, improper implementation of mechanisms to prevent DOS attacks.
Unauthorized access, network reconnaissance
Unauthorized infrastructure access, administrative privileges exploitation
Unauthenticated arbitrary file disclosure

Threat Name
DOS attacks, Arbitrary code execution slow system memory leak
Remote code execution, Flood attacks to harm system’s availability.
Loss of Data Privacy and Confidentiality, Retrieval of unauthorized data and Man-In-The-Middle attack

Full control of architecture, unable to access any machine.
Buffer overflows attacks

Risks
Exhaustion of resources of affected systems, memory exhaustion resulting in unexpected reloads.
Full system compromise, Manipulation of sensitive information in lo files.
Weak network infrastructure, attackers maintain persistence within the network
loss of control of infrastructure backbone,
unauthorized access might result in damage and installation of malware on systems.

Database Security Risk Management Implementation Controls and Policies

a. Authentication – User accounts
b. Authorization
c. Confidentiality
d. Data Integrity
e. Auditing
f. Replication and Federation
g. Clustering
h. Backup and Recovery
i. OS Protections
j. Application protections
k. Network protections
l. Security Design and Configuration
m. Enclave and Computing environment
n. Business Continuity
o. Vulnerability and Incident management

The following are the list of critical assets present in Symetrica:

ASSET	**ASSET NAME**	Asset Value
A1	Backbone Switch	$15,000
A2	Cable Modem	$35,000
A3	Switches (X4)	$20,000
A4	W Access Points (X5)	$25,000
A5	**MISys** (maintains inventory)	$75,000
A6	**Symetrica US Server-03**	$100,000
A7	**Arena** (all data and processes tied to the product)	$50,000

A11	QNAP NAS	$65,000
A12	UPS	$30,000
A13	**Firewall Sophos-XG-125**	$55,000
A14	AWS Fleet Servers and services	$30,000
A15	**Gitlab** services	$15,000
A16	Jenkins/Builder	$45,000
A17	PC's	$85,000
A18	Printers	$20,000
A19	Phabricator	$60,000
A20	Internal Correspondence	Intangible
A21	Personnel Information	Intangible
A22	Contracting and Procurement Documents	Intangible
A23	Reputation (Intangible)	Intangible
A24	Employee Confidence (Intangible)	Intangible

List of missing controls:

Missing Controls
Certificates
External Authentication
Encryption of Application Code
Transaction Log
Audit log protection
Audit log retention
Database Clustering
Testing and Mainatnence
Dedicated operating systems account
Audit of elevated privileges
Least privilege mechanism

Vulnerability Name
Exploitation of Buffer Overflow Vulnerability
Lack of encrypted communications resulting in Unauthorized access,
network reconnaissance and Unauthenticated arbitrary file disclosure
Failure to apply patches and updates and neglected databases

Threats
DOS attacks, Injection attacks
Identity theft, brute-force attack and social engineering schemes

Retrieval of unauthorized data andd Man-In-The-Middle attack
Full control of architecture, unable to access any machine.
Buffer overflows attacks

Risks
Exhaustion of resources due to submission of malformed queries.
Privilege escalation, Full system compromise
Weak network infrastructure, escalation of level of attack
loss of control of infrastructure backbone,
Unnecessary privileges might result in unauthorized access might result in damage and installation of malware on systems.

Applications Development Security Risk Management Implementation Controls and Policies

a. Program Management
b. Application Data Handling
c. Authentication
d. Use of Cryptography
e. User Accounts
f. Input Validation
g. Auditing
h. Configuration Management
i. Testing
j. Deployment

The following are the list of critical assets present in Symetrica:

ASSET	**ASSET NAME**	Asset Value
A1	Backbone Switch	$15,000
A2	Cable Modem	$35,000
A3	Switches (X4)	$20,000
A4	W Access Points (X5)	$25,000
A5	**MISys** (maintains inventory)	$75,000
A6	**Symetrica US Server-03**	$100,000
A7	**Arena** (all data and processes tied to the product)	$50,000
A11	QNAP NAS	$65,000

A12	UPS	$30,000
A13	**Firewall Sophos-XG-125**	$55,000
A14	AWS Fleet Servers and services	$30,000
A15	**Gitlab** services	$15,000
A16	Jenkins/Builder	$45,000
A17	PC’s	$85,000
A18	Printers	$20,000
A19	Phabricator	$60,000
A20	Internal Correspondence	Intangible
A21	Personnel Information	Intangible
A22	Contracting and Procurement Documents	Intangible
A23	Reputation (Intangible)	Intangible
A24	Employee Confidence (Intangible)	Intangible

List of missing controls:

Missing Controls
Application Data Handling
Data Transmission
Data Marking
Authentication
User Authentication
Signed Code Identification
Standalone Application Authentication
Combination Client Server Application Authentication
Application Component Authentication
PKI Certificate Validation
Authentication Credentials Protections
Use of Cryptography
Message authentication Code
Digital Signatures
User Accounts
Application account handling
Account locks
Input Validation
Web Encoding
Race Condition
Auditing
Protecting audit trails
Deployment
Documentation
Auditing

Vulnerability Name
Cipher transmission insecure, sensitive data exposure.
Installation of malware, improper certificate validation,
Broken authentication, Session ID leakage, Unrestricted file uploads
Directory indexing, insufficient session expiration
Excess privilege assigned to accounts, security misconfigurations,
Unvalidated automatic library activation, Insufficient auditing and logging.

Threat Name
Credential theft attacks, information theft
Illegitimate data transfer attacks, Denial of Service attacks.
Unauthorized access, Credential theft attacks
Elevated privileges attacks, Credential theft attacks, Data interception
Server and other critical assets attacks, Malware or other malicious code uploads.

Risks
Escalated root access, user accounts data exposure.
Installation of malware on endpoints, manipulation of data.
unauthorized access might result in damage and failed access controls
Remote code execution, inability to identify the breach
Unauthorized folders and data access, read, update or delete data

Wireless Security Risk Management Implementation Controls and Policies

a. Wireless LAN Risk Management
b. Wireless PAN Risk Management
c. Wireless WAN Risk Management
d. Wireless RFID Risk Management
e. Wireless PED Risk Management

The following are the list of critical assets present in Symetrica:

ASSET	**ASSET NAME**	Asset Value
A1	Backbone Switch	$15,000
A2	Cable Modem	$35,000
A3	Switches (X4)	$20,000
A4	W Access Points (X5)	$25,000
A5	**MISys** (maintains inventory)	$75,000
A6	**Symetrica US Server-03**	$100,000
A7	**Arena** (all data and processes tied to the product)	$50,000
A11	QNAP NAS	$65,000
A12	UPS	$30,000
A13	**Firewall Sophos-XG-125**	$55,000
A14	AWS Fleet Servers and services	$30,000
A15	**Gitlab** services	$15,000
A16	Jenkins/Builder	$45,000
A17	PC's	$85,000
A18	Printers	$20,000
A19	Phabricator	$60,000
A20	Internal Correspondence	Intangible
A21	Personnel Information	Intangible
A22	Contracting and Procurement Documents	Intangible
A23	Reputation (Intangible)	Intangible
A24	Employee Confidence (Intangible)	Intangible

List of missing controls:

Missing Controls
Wireless LAN Risk Management
EAP- Transport Layer Security
EAP-Tunneling Transport Layer Security
Protected Extensible Authentication Protocol
RSN, WRAP and CCMP Protocols
Wireless PAN Risk Management
Device Level Authentication
Data Encryption
Security Modes and Levels
Key Management
Wireless WAN Risk Management
Cellular Digital Packet Data Protocol (CDPD)
Mobitex
WiMax
Wireless RFID Risk Management
Radio Frequency Identification Encryption
Wireless PED Risk Management

PDA Security

Vulnerability Name
Wireless Zero Configuration vulnerability, Rogue Access Points vulnerability
Bluetooth exploits.
Cloning vulnerability and password disclosures. Vulnerabilities related to non-encrypted 802.11 traffic
Sensitive data disclosure, autorun feature vulnerabilities

Threat Name
Sniffing and wireless scanning attacks, piggybacking & network reconnaissance Attacks
Blue-snarfing, Blue-bugging, Blue-jacking and Bluetooth Dos attacks.
Evil Twin attacks, Retrieval of unauthorized data and Man-In-The-Middle attack
Outbound email attacks and Eavesdropping attacks.

Risks
Manipulation of DNS server settings, mounting malicious firmware on routers, giving full access to the attacker.
Infect systems laterally connected and block legitimate Bluetooth traffic.
Masquerading as an authorized user & data modification
unauthorized access might result in damage and installation of malware on systems.

List of Cybersecurity Implementation controls that exist Symetrica:

Access Control Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls
Identification Controls
Employee Card
Password

PKI Certificates
Digital Certificates
Authentication
Badge
Key
Smart Card
Password
Authorization
Access Control Lists
Deny-by-default Policy
Logical Access Control Methods:
Network Architecture Controls
Remote Network Access
Logical Network Port Security
Network Access Control Systems
Encryption
Authentication Factors
Passwords
PINs
Physical Access Control Methods
Classified Storage and Handling
Attended Access
Smart Cards
PINS
Physical Intrusion Detection Systems
Badges

Network Infrastructure Security Risk Management Implementation Controls and Policies

Enclave Protection
Firewalls
Routers/ Switches
Intrusion Prevention System
Restricted LAN Segment
No Backdoor connections
Firewalls
Deep packet Inspection

Network Infrastructure Management Security Risk Management Implementation Controls and Policies:

Implementation Controls
Ports, Protocols & Services

Denying/Dropping protocols
Block Traceroute utility
IPv4 & IPv6 Address Filtering
Device Management
Device Vulnerability Management System
Device Monitoring
SNMP
Network Management Station
Network Authentication, Authorization, and Accounting
Authentication
Authorization
Network Intrusion Detection System (NIDS)
External NIDS
Switches and VLANs
Physical Switches and Wiring
Virtual Local Area Networks (VLANs)
VLAN Trunking
Virtual Private Network
Gateway to Gateway
Host to the gateway

Database Security Risk Management Implementation Controls and Policies:

AUTHENTICATION:
User Accounts:
Database Administrator (DBA)
Application Owner
Access Control Lists
Credentials storage:
Encryption of application code:
REPLICATION AND FEDERATION
Database links
Database clustering
Principle of least privilege:
Test plans and procedures
Trail of accountability:
Protected communication path:
BACKUP AND RECOVERY
DBMS backup:
OS PROTECTIONS
Dedicated directories and files:
Updated database software:

APPLICATION PROTECTIONS
Input validation
Authentication method
NETWORK PROTECTIONS
Network Access
Time and Count limits
Encrypted and protected data across network
SECURITY DESIGN AND CONFIGURATION
Procedural Review
Configural Specification
Compliance Testing
Functional architecture for IS applications
Nonrepudiation
Partitioning the application
Ports, protocols and services
Configuration management process
System library management controls
Software baselines
Individual identification and authentication
Key management
ENCLAVE AND COMPUTING ENVIRONMENT
Audit record content
Audit monitoring, analysis and reporting
Privileged account control
Marking and Labeling
Production code Change Controls
Resource control
Security Configuration Compliance
Audit reduction and report generation
BUSINESS CONTINUITY:
Protection backup and restoration assets
Data backup procedures
Disaster recovery and planning
VULNERABILITY AND INCIDENT MANAGEMENTR
Vulnerability management

Applications Development Security Risk Management Implementation Controls and Policies

Application Data Handling:
Database Management System
Data Storage
In-memory Data Handling
Data Integrity

Authentication:
Server Authentication
Server Application Authentication
Client Application Authentication
Password Complexity and Maintenance
Use of Cryptography:
Symmetric Encryption
Input Validation:
User Input Validation
Static Analysis
Sensitive Information Disclosure
Auditing:
Notification and audit content
Configuration Management:
Software configuration management
Limit unauthorized individuals
Testing:
Test plans and procedures

Wireless Security Risk Management Implementation Controls and Policies

Wireless LAN Risk Management
IEEE 802.11x Extensible Authentication Protocol
Separation of Network:
VPN:
User Authentication and Data Encryption Services:
Wi-Fi protected access:
Service Set Identifier:
Access point and client identification:
Wireless PAN Risk Management:
Bluetooth Specification
Pairing or Bonding
Confidentiality, Integrity, Authentication and Authorization
Secure simple pairing
Wireless WAN Risk Management
Broadband Wireless Access

Wireless PED Risk Management:
Subscriber Identity Module cards
Wireless Email

Comparison of the Implementation controls discussed in class with Symetrica's existing Cybersecurity Implementation controls

Access Control Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls	Implementation Status
Identification Controls	
Employee Card	Present
Password	Present
PKI Certificates	Present
Digital Certificates	Present
Biometric Feature	Absent
Authentication	
Badge	Present
Key	Present
Smart Card	Present
Password	Present
Fingerprint Verification	Absent
Hand Geometry	Absent
PKI Certificate	Present
Cryptographic Hardware Token	Absent
Authorization	
Access Control Lists	Present
Security Tokens	Absent
Deny-by-default Policy	Present
Logical Access Control Methods:	
Network Architecture Controls	Present
Remote Network Access	Present
Physical Security for SIPRNeT ports	Absent

Logical Network Port Security	Present
Port Authentication using 802.1X	Absent
Network Access Control Systems	Present
Encryption	Present
Authentication Factors	Present
PKI Compliance Requirements	Absent
Passwords	Present
PINs	Present
Physical Access Control Methods	
Classified Storage and Handling	Present
Attended Access	Present
Memory Cards	Absent
Smart Cards	Present
PINS	Present
Physical Tokens	Absent
Physical Intrusion Detection Systems	Present
Badges	Present
Biometric Systems:	
Fingerprint Reader	Absent
Hand Geometry Reader	Absent
Iris Scanner	Absent

Network Infrastructure Security Risk Management Implementation Controls and Policies

Enclave Protection	
Firewalls	Present
Routers/ Switches	Present
Intrusion Detection System	Absent
Intrusion Prevention System	Present
Demilitarized Zone	Absent
Approved Gateways	Absent
Network Test Access Ports	Absent
Restricted LAN Segment	Present
Wireless IDS	Absent
No Backdoor connections	Present
Firewalls	
Packet filter	Absent
Bastion Host	Absent
Stateful Inspection	Absent
Deep packet Inspection	Present
Application Proxy Gateway	Absent
Hybrid Technology Firewalls	Absent
Proxy Servers	Absent

Routers:	
Route Table Integrity:	N/A
Router Planes	N/A

Network Infrastructure Management Security Risk Management Implementation Controls and Policies

Implementation Controls	**Implementation Status**
Ports, Protocols & Services	
Denying/Dropping protocols	Present
Restricting ICMPv4 message	Absent
Block Traceroute utility	Present
IPv4 & IPv6 Address Filtering	Present
Unicast Reverse Path Forwarding	Absent
Protection against SYN Flood Attack	Absent
Device Management	
Device Vulnerability Management System	Present
Out-of-band device management	Absent
In-band device management	Absent
Device Monitoring	
SNMP	Present
Network Management Station	Present
Network Authentication, Authorization, and Accounting	
Authentication	Present
Authorization	Present
Accounting	Absent
Auditing	Absent
Router Password Protection	Absent
Network Intrusion Detection System (NIDS)	
Local Area NIDS	Absent
External NIDS	Absent
Switches and VLANs	
Physical Switches and Wiring	Present
Virtual Local Area Networks (VLANs)	Present
VLAN Trunking	Present
VLAN Port Security	Absent
VLAN 802.1x and Management Policy Server	Absent
Virtual Private Network	
Gateway to Gateway	Present

Host to host	Absent
Host to the gateway	Present

Database Security Risk Management Implementation Controls and Policies

AUTHENTICATION	
User Accounts:	PRESENT
Database Administrator (DBA)	PRESENT
Application Owner	PRESENT
Application User Manager	ABSENT
Application Accounts	PRESENT
Database Auditor	ABSENT
Database Operator	
Access Control Lists	PRESENT
Passwords	ABSENT
Certificates:	ABSENT
External Authentication	ABSENT
Credentials storage:	PRESENT
AUTHORIZATION	ABSENT
Role based access controls:	ABSENT
Renaming default accounts:	ABSENT
CONFIDENTIALITY	ABSENT
Data encryption:	
Encryption of application code:	PRESENT
Data file encryption:	ABSENT
DATA INTEGRITY	
Transaction log:	ABSENT
Data integrity:	ABSENT
AUDITING	PRESENT
Audit log protection	ABSENT
Audit log retention	ABSENT
REPLICATION AND FEDERATION	PRESENT
Database replication	
Database links	PRESENT
CLUSTERING	
Database clustering	PRESENT
Principle of least privilege:	PRESENT
Testing:	
Test plans and procedures	PRESENT
Deployment:	
Documentation	ABSENT
Auditing	ABSENT
Trail of accountability:	PRESENT
Protected communication path:	PRESENT

BACKUP AND RECOVERY	
DBMS backup:	PRESENT
Testing and maintenance:	ABSENT
Authentication and authorization:	ABSENT
OS PROTECTIONS	
Dedicated directories and files:	PRESENT
Dedicated operating systems account:	ABSENT
Updated database software:	PRESENT
APPLICATION PROTECTIONS	
Audit of elevated privileges:	ABSENT
Input validation	PRESENT
Authentication method	PRESENT
Least privilege mechanism:	ABSENT
NETWORK PROTECTIONS	
Network Access	PRESENT
Time and Count limits	PRESENT
Encrypted and protected data across network	PRESENT
SECURITY DESIGN AND CONFIGURATION	
Procedural Review	PRESENT
Configural Specification	PRESENT
Compliance Testing	PRESENT
Functional architecture for IS applications	PRESENT
Nonrepudiation	PRESENT
Partitioning the application	PRESENT
Ports, protocols and services	PRESENT
Configuration management process	PRESENT
IA documentation	ABSENT
System library management controls	PRESENT
System state changes	ABSENT
Software baselines	PRESENT
Group identification and authentication	ABSENT
Individual identification and authentication	PRESENT
Key management	PRESENT
Token and certificate standards	ABSENT
ENCLAVE AND COMPUTING ENVIRONMENT	
Access for need to know	ABSENT
Audit record content	PRESENT
Audit monitoring, analysis and reporting	PRESENT
Privileged account control	PRESENT
Marking and Labeling	PRESENT
Production code Change Controls	PRESENT
Resource control	PRESENT
Security Configuration Compliance	PRESENT
Audit reduction and report generation	PRESENT
Software development change controls	ABSENT

Warning message	ABSENT
Boundary defense	ABSENT
Remote access for privilege functions	ABSENT
BUSINESS CONTINUITY:	
Protection backup and restoration assets	PRESENT
Data backup procedures	PRESENT
Disaster recovery and planning	PRESENT
Backup copy of critical data	ABSENT
Trusted recovery	ABSENT
VULNERABILITY AND INCIDENT MANAGEMENTR	
Vulnerability management	PRESENT

Applications Development Security Risk Management Implementation Controls and Policies

Application Data Handling:	
Database Management System	PRESENT
Data Storage	PRESENT
In-memory Data Handling	PRESENT
Data Transmission	ABSENT
Data Integrity	PRESENT
Data Marking	ABSENT
Authentication:	
Server Authentication	PRESENT
User Authentication	ABSENT
Signed Code Identification	ABSENT
Standalone Application Authentication	ABSENT
Server Application Authentication	PRESENT
Client Application Authentication	PRESENT
Combination Client Server Application Authentication	ABSENT
Application Component Authentication	ABSENT
PKI Certificate Validation	ABSENT
Password Complexity and Maintenance	PRESENT
Authentication Credentials Protections	ABSENT
Use of Cryptography:	
Symmetric Encryption	PRESENT
Message authentication Code	ABSENT
Digital Signatures	ABSENT
User Accounts:	
Application account handling	ABSENT
Account locks	ABSENT
Input Validation:	
User Input Validation	PRESENT
Web Encoding	ABSENT

Race Condition	ABSENT
Static Analysis	PRESENT
Sensitive Information Disclosure	PRESENT
Auditing:	
Notification and audit content	PRESENT
Protecting audit trails	ABSENT
Configuration Management:	
Software configuration management	PRESENT
Limit unauthorized individuals	PRESENT
Testing:	
Test plans and procedures	PRESENT
Deployment:	
Documentation	ABSENT
Auditing	ABSENT

Wireless Security Risk Management Implementation Controls and Policies

Wireless LAN Risk Management	
IEEE 802.11x Extensible Authentication Protocol	PRESENT
EAP- Transport Layer Security	ABSENT
EAP-Tunneling Transport Layer Security	ABSENT
Protected Extensible Authentication Protocol	ABSENT
Separation of Network:	PRESENT
VPN:	PRESENT
User Authentication and Data Encryption Services:	PRESENT
Wi-Fi protected access:	PRESENT
Service Set Identifier:	PRESENT
Access point and client identification:	PRESENT
RSN, WRAP and CCMP Protocols:	ABSENT
Wireless PAN Risk Management:	
Bluetooth Specification	PRESENT
Device Level Authentication	ABSENT
Data Encryption	ABSENT
Pairing or Bonding	PRESENT
Confidentiality, Integrity, Authentication and Authorization	PRESENT
Security Modes and Levels	ABSENT
Secure simple pairing	PRESENT
Key Management	ABSENT
Wireless WAN Risk Management	
Cellular Digital Packet Data Protocol (CDPD)	ABSENT
Mobitex	ABSENT

Broadband Wireless Access	PRESENT
WiMAX	ABSENT
Wireless RFID Risk Management:	
Radio Frequency Identification Encryption	ABSENT
Wireless PED Risk Management:	
Subscriber Identity Module cards	PRESENT
Wireless Email	PRESENT
PDA Security	ABSENT

List of critical assets present at Symetrica:

ASSET NAME
Backbone Switch
Cable Modem
Switches (X4)
W Access Points (X5)
MISys (maintains inventory)
Symetrica US Server-03
Arena (all data and processes tied to the product)
QNAP NAS
UPS
Firewall Sophos-XG-125
AWS Fleet Servers and services
Gitlab services
Jenkins/Builder
PC’s
Printers
Phabricator
Internal Correspondence
Personnel Information
Contracting and Procurement Documents
Reputation (Intangible)
Employee Confidence (Intangible)

List of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing

- Vulnerabilities Related to authentication logic and Insecure session handling
- vulnerabilities related to internal corporate attacks and disclosure or brokerage of information
- Unauthorized Access and missing lock out process
- Vulnerabilities related to Unauthorized Access, Vulnerabilities Related to Interruption of Operations
- Vulnerabilities Related to access control, vulnerabilities related to IP addresses, ports and services disclosure.
- vulnerabilities related to malicious traffic, website breaches and data exfiltration
- Rogue WIFI Access Points (WAPS), Vulnerabilities related to non-encrypted 802.11 traffic
- Private IP Address disclosure, malicious software related attacks
- Improper memory resource management, missing input validation, improper error handling
- Improper filtration of serialized input, improper implementation of mechanisms to prevent DOS attacks.
- Unauthorized access, network reconnaissance
- Unauthorized infrastructure access, administrative privileges exploitation
- Unauthenticated arbitrary file disclosure

- Cipher transmission insecure, sensitive data exposure.
- Installation of malware, improper certificate validation,
- Broken authentication, Session ID leakage, Unrestricted file uploads
- Directory indexing, insufficient session expiration
- Excess privilege assigned to accounts, security misconfigurations,
- Unvalidated automatic library activation, Insufficient auditing and logging.
- Wireless Zero Configuration vulnerability, Rogue Access Points vulnerability
- Bluetooth exploits.
- Cloning vulnerability and password disclosures. Vulnerabilities related to non-encrypted 802.11 traffic
- Sensitive data disclosure, autorun feature vulnerabilities

List of potential threats to Symetrica that could exploit vulnerabilities of critical assets

- Operating System and escalated privileges Attacks
- Manual exploitation of logical flaws and Heap Buffer Overflow Attacks
- Retrieval of unauthorized data and Man-In-The-Middle attack

- Retrieval of unauthenticated data and overriding authenticated sessions- session hijacking
- Brute force attacks, user enumeration and denial of service attacks
- network reconnaissance and IP spoofing, escalated privileges Attacks
- DDOS attack, cross site scripting and SQL injection attacks
- Outbound email attacks, Threats related to downloads to insecure devices, uploads to cloud storage and unsecured behavior in cloud
- Retrieval of unauthorized data and Man-In-The-Middle attack
- Network Layer attacks, social engineering attacks, retrieval of unauthenticated data, website cookie exploitation and overriding authenticated sessions- session hijacking
- DOS attacks, Arbitrary code execution slow system memory leak
- Remote code execution, Flood attacks to harm system's availability.
- Loss of Data Privacy and Confidentiality, Retrieval of unauthorized data and Man-In-The-Middle attack
- Full control of architecture, unable to access any machine.
- Buffer overflows attacks
- Credential theft attacks, information theft
- Illegitimate data transfer attacks, Denial of Service attacks.
- Unauthorized access, Credential theft attacks
- Elevated privileges attacks, Credential theft attacks, Data interception
- Server and other critical assets attacks, Malware or other malicious code uploads.
- Sniffing and wireless scanning attacks, piggybacking & network reconnaissance Attacks
- Blue-snarfing, Blue-bugging, Blue-jacking and Bluetooth Dos attacks.
- Evil Twin attacks, Retrieval of unauthorized data and Man-In-The-Middle attack
- Outbound email attacks and Eavesdropping attacks.

List of potential risks for critical assets where Cybersecurity Implementation Controls are missing

- Cause interruption of operations due to authenticating non trusted access
- Result in operating system attacks and unavailability of services
- Result in network related attacks, improper functioning of infrastructure & non-compliance
- Unauthorized Access might result in damage and loss of physical assets
- Deteriorating the throughput of network's links, possibility of DOS attacks and unavailability of services
- Loss of Personally Identified Information, Breaches on FTP and HTTPS sites, attacks related to accepting uploaded data.
- Masquerading as an authorized user, data modification and creation of backdoors to internal network due to rogue APs.
- Data Breaches, unauthorized access might result in damage and installation of malware on systems.
- Exhaustion of resources of affected systems, memory exhaustion resulting in unexpected reloads.

- Full system compromise, Manipulation of sensitive information in lo files.
- Weak network infrastructure, attackers maintain persistence within the network
- loss of control of infrastructure backbone,
- unauthorized access might result in damage and installation of malware on systems.
- Escalated root access, user accounts data exposure.
- Installation of malware on endpoints, manipulation of data.
- unauthorized access might result in damage and failed access controls
- Remote code execution, inability to identify the breach
- Unauthorized folders and data access, read, update or delete data
- Manipulation of DNS server settings, mounting malicious firmware on routers, giving full access to the attacker.
- Infect systems laterally connected and block legitimate Bluetooth traffic.
- Masquerading as an authorized user & data modification
- unauthorized access might result in damage and installation of malware on systems.

List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks. – Risk Prevention Strategy

- Security Awareness Training programs highlighting the higher probability threats can be made more frequent.
- Authorize Processing (Certification and Accreditation) controls needs to be implemented to prevent from trusting non-authorized parties.
- Efficient controls relating to Contingency Planning and Division contingency planning need to be implemented.
- For Unauthorized Access additional hardening controls can be implemented to mitigate "in the clear" conversations.
- Implementation of Multi Factor Authentication with biometrics/ security device can also help to mitigate vulnerabilities to greater extent.
- Implement principle of least privilege and limit lateral communication between PC's and management interfaces.
- Disable remote admin network protocols such as FTP, Telnet and safeguard configuration files using encryption or access controls during transit, storage, and back up of files.
- Separate the management traffic and manage the privileged access by using a server that provides authentication, authorization and accounting services to assign privileges and store access information.
- Ensure that management traffic uses Out of Bound Management to remotely manage the devices and apply encryption on all remote access, management traffic to devices such as terminals and dial in servers.
- Use host-based firewalls on critical devices to restrict communications from other hosts on network. Harden the network management devices by using strong password policies and disabling unnecessary management services on the devices.
- Separate the network traffic traversing through the same router by implementing Virtual Routing & Forwarding technology and implement Virtual Access Control Lists to control the ingress and egress traffic from VLANs.
- Secure access to the consoles, routers, and switches by controlling remote administration access and implement robust password policies for stronger authentication.
- Separate the management traffic from the network traffic and encrypt all administrative communications.
- Test patches, restrict unnecessary administrative or management services and periodically test the security configurations against security requirements.
- Implement Enforcement of Multi-Factor Authentication on any account that is accessible via internet and implementation of principle of least privilege to provide necessary privileges is necessary.
- Implement separation of network, such as moving the servers and application accessible via internet to DMZ can help to prevent lateral movement of attacks.
- For the data in transit, disable implementation weak cyphers such as SSLv2, 3DES, disable any HTTP communication and allow only HTTPS or HSTS communication.

- Scan for any configuration and software vulnerabilities and patch all the high and critical vulnerabilities within 15-30 days for internet accessible systems and applications.
- Implement AES CCMP or above encryption protocols for WPA-2 enterprise networks.
- Implement Rogue client detection capability, rogue WAP detection capability, rogue process detection capability to detect the presence of malicious workstations, rogue access points and rogue devices and services for over-the-air and wired communications.
- Implement “no-Wi-Fi” and “Acceptable Bluetooth use” policies per subnet and across all subnets for defense-in-depth approach.
- The communication between the server and the access points should be as minimal as possible and the communication should be classified for all the clients and WAP’s with minimal KBPS traffic identified for them.
- Configuration management, user awareness training and Bluetooth awareness policy shall help mitigate Bluetooth related risks to greater extent.

List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience **– Risk Response Strategy**

- Controls strengthening Incident Response Capabilities need to be implemented.
- Periodically reviewing the effectiveness of Security Controls can help strengthen the controls in place and reduce the probabilities of vulnerabilities.
- Intrusion Prevention Systems and regular update of digital signatures need to be done to proactively mitigate uprising threats.
- Patches need to be regularly checked, tested in an isolated environment and patched.
- Audit Trails control can be implemented and reviewed to identify potential service and process problems.
- Intermittently test the security configurations, backup the configurations and store them offline.
- Continually monitor and assess the security of management and critical systems, networks and infrastructure.
- Test backups of the system consistently and schedule operating system patches and hardware firmware patches at routine intervals.
- SIEM technology can be integrated to integrate multiple log formats from different sources and generate alerts on identified traffic patterns.
- By applying such various countermeasures, it is also necessary to test the incident response plan periodically to evaluate the effectiveness and update the plan accordingly.
- Monitor and log networking devices and verify their configurations schedule periodically.

- Manage and store the access information of networking devices by using Authentication, Authorization and Accounting services, to limit the access and only required privileges to the user.
- Document, review and update the Disaster recovery, Business continuity and continency plans.
- Reviewing and monitoring the log files of networking devices, can help in identifying potential exploitation attempts, to harden the networking devices
- Implement backup solutions to automatically back up critical data and keep the backup data in a secure and remotely isolated environment.
- Implement security checklist to audit and harden the application configurations and allow only the application modules and services that are required as per business needs.
- Implement Cross-Site Scripting and Cross-Site Scripting forgery protections to prevent from the most common attacks.
- Audit the code and services that are being provided by third-party while not being hosted on the server to ensure that there is no invalidated code being delivered.
- Blocking the most commonly exploited wireless attacks identified in this plan along with detection and reporting of any additional attacks can strengthen the prevention control capabilities.
- Generate automated event triggering, event log capturing and creation of customizable reports.
- Implementation of Wireless Intrusion Prevention/ Detection Systems to detect and classify various devices supporting 802.11 standards connected to wired and wireless networks.
- Implement MFA and EAP-TLS certificate or above based methods to ensure secure authentication for wireless transactions.

Applicable Government Regulations and Industry Standards

Cyber Essentials Scheme

This is UK Government assurance scheme providing the baseline for cybersecurity posture by implementation of five cybersecurity controls. These five security controls address the following:

- Access control
- secure configuration
- firewalls and Internet gateways
- patch management
- malware protection.

The Cyber Essentials plus provides the cybersecurity measures to be adopted by all sizes of the organization. Symetrica is required to be compliant with CES to continue working on all government related contracts.

ISO 27001

This standard is part of the family of ISO 27K Standards that provides generic security controls for secure design and implementation Information System Management System. ISO27001 has a list of 114 security controls providing the specifications and details the requirements for Information System Management System. This standard also lays out the controls for risk management processes, cost effective risk management implementation, information system monitoring activities and security investments for the risk-based decisions.

NIST 800-171

This is a publication that lays out the standards and controls for organizations that control the DoD Controlled Unclassified Information. The NIST 800-171 consists of 110 seecurity controls that address the following:

- Access control
- Awareness and Training
- Audit and Accountability
- Configuration Management
- Identification and Authentication
- Incident Response
- Maintenance
- Media Protection
- Personnel Security
- Physical Protection
- Risk Assessment
- Security Assessment
- System and Communication Protection
- System and Communication Protection

Rank asset risks and vulnerability risks for your company across Access Control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless.

Risk Management Areas	Risks	Vulnerabilities
Access Control	Might cause interruption of operations due to authenticating non trusted access	Vulnerabilities Related to authentication logic and Insecure session handling
	It might result in operating system attacks and unavailability of services	vulnerabilities related to internal corporate attacks
	It might result in network related attacks	Unauthorized Access and missing lock out process
	Unauthorized Access might result in damage and loss of physical assets	Vulnerabilities related to Unauthorized Access
	improper functioning of infrastructure & non-compliance	Vulnerabilities Related to disclosure or brokerage of information
Network Risk	Deteriorating the throughput of network's links, possibility of DOS attacks and unavailability of services	Vulnerabilities Related to access control
	Loss of Personally Identified Information, Breaches on FTP and HTTPS sites, attacks related to accepting uploaded data.	vulnerabilities related to malicious traffic, website breaches and data exfiltration
	Masquerading as an authorized user, data modification and creation of backdoors to internal network due to rogue APs.	Rogue WIFI Access Points (WAPS), Vulnerabilities related to non-encrypted 802.11 traffic
	Data Breaches, unauthorized access might result in damage	Private IP Address disclosure, malicious software related attacks
	installation of malware on systems.	vulnerabilities related to IP addresses, ports, and services disclosure.
	Exhaustion of resources of affected systems, memory exhaustion resulting in unexpected reloads.	Improper memory resource management, missing input validation, improper error handling

Network Risk	Full system compromise, Manipulation of sensitive information in lo files.	Improper filtration of serialized input, improper implementation of mechanisms to prevent DOS attacks.
	Weak network infrastructure, attackers maintain persistence within the network	Unauthorized access, network reconnaissance
	loss of control of infrastructure backbone,	Unauthorized infrastructure access, administrative privileges exploitation
	unauthorized access might result in damage and installation of malware on systems.	Unauthenticated arbitrary file disclosure
Database Risk Management	Exhaustion of resources due to submission of malformed queries.	Exploitation of Buffer Overflow Vulnerability
	Privilege escalation, Full system compromise	Lack of encrypted communications resulting in Unauthorized access,
	Weak network infrastructure, escalation of level of attack	network reconnaissance and Unauthenticated arbitrary file disclosure
	loss of control of infrastructure backbone,	Failure to apply patches and updates and neglected databases
	improper functioning of infrastructure & non-compliance	Vulnerabilities Related to disclosure or brokerage of information
Application Risk Management	Escalated root access, user accounts data exposure.	Cipher transmission insecure, sensitive data exposure.
	Installation of malware on endpoints, manipulation of data.	Installation of malware, improper certificate validation,
	unauthorized access might result in damage and failed access controls	Broken authentication, Session ID leakage, Unrestricted file uploads
	Remote code execution, inability to identify the breach	Directory indexing, insufficient session expiration

	Unauthorized folders and data access, read, update or delete data	Excess privilege assigned to accounts, security misconfigurations,
Wireless Risk Management	Manipulation of DNS server settings, mounting malicious firmware on routers, giving full access to the attacker.	Wireless Zero Configuration vulnerability
	Infect systems laterally connected and block legitimate Bluetooth traffic.	Bluetooth exploits.
	Masquerading as an authorized user	Cloning vulnerability and password disclosures. Vulnerabilities related to non-encrypted 802.11 traffic
	unauthorized access might result in damage	Sensitive data disclosure, autorun feature vulnerabilities
	data modification and installation of malware on systems.	Rogue Access Points vulnerability

List of top 5 Vulnerabilities:

1. Unauthorized infrastructure access, administrative privileges exploitation
2. Vulnerabilities related to Unauthorized Access
3. Installation of malware, improper certificate validation
4. Rogue WIFI Access Points (WAPS), Vulnerabilities related to non-encrypted 802.11 traffic
5. Sensitive data disclosure, autorun feature vulnerabilities

List of top 5 Risks:

1. loss of control of infrastructure backbone
2. Weak network infrastructure, attackers maintain persistence within the network
3. Remote code execution, inability to identify the breach
4. Might cause interruption of operations due to authenticating non trusted access
5. Loss of Personally Identified Information, Breaches on FTP and HTTPS sites, attacks related to accepting uploaded data.

List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks. – Risk Prevention Strategy

- Security Awareness Training programs highlighting the higher probability threats can be made more frequent.
- Authorize Processing (Certification and Accreditation) controls needs to be implemented to prevent from trusting non-authorized parties.
- Efficient controls relating to Contingency Planning and Division contingency planning need to be implemented.
- For Unauthorized Access additional hardening controls can be implemented to mitigate "in the clear" conversations.
- Implementation of Multi Factor Authentication with biometrics/ security device can also help to mitigate vulnerabilities to greater extent.
- Implement principle of least privilege and limit lateral communication between PC's and management interfaces.
- Disable remote admin network protocols such as FTP, Telnet and safeguard configuration files using encryption or access controls during transit, storage, and back up of files.
- Separate the management traffic and manage the privileged access by using a server that provides authentication, authorization and accounting services to assign privileges and store access information.
- Ensure that management traffic uses Out of Bound Management to remotely manage the devices and apply encryption on all remote access, management traffic to devices such as terminals and dial in servers.
- Use host-based firewalls on critical devices to restrict communications from other hosts on network. Harden the network management devices by using strong password policies and disabling unnecessary management services on the devices.
- Separate the network traffic traversing through the same router by implementing Virtual Routing & Forwarding technology and implement Virtual Access Control Lists to control the ingress and egress traffic from VLANs.
- Secure access to the consoles, routers, and switches by controlling remote administration access and implement robust password policies for stronger authentication.
- Separate the management traffic from the network traffic and encrypt all administrative communications.
- Test patches, restrict unnecessary administrative or management services and periodically test the security configurations against security requirements.
- Implement Enforcement of Multi-Factor Authentication on any account that is accessible via internet and implementation of principle of least privilege to provide necessary privileges is necessary.
- Implement separation of network, such as moving the servers and application accessible via internet to DMZ can help to prevent lateral movement of attacks.
- For the data in transit, disable implementation weak cyphers such as SSLv2, 3DES, disable any HTTP communication and allow only HTTPS or HSTS communication.

- Scan for any configuration and software vulnerabilities and patch all the high and critical vulnerabilities within 15-30 days for internet accessible systems and applications.
- Implement AES CCMP or above encryption protocols for WPA-2 enterprise networks.
- Implement Rogue client detection capability, rogue WAP detection capability, rogue process detection capability to detect the presence of malicious workstations, rogue access points and rogue devices and services for over-the-air and wired communications.
- Implement "no-Wi-Fi" and "Acceptable Bluetooth use" policies per subnet and across all subnets for defense-in-depth approach.
- The communication between the server and the access points should be as minimal as possible and the communication should be classified for all the clients and WAP's with minimal KBPS traffic identified for them.
- Configuration management, user awareness training and Bluetooth awareness policy shall help mitigate Bluetooth related risks to greater extent.

List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience **– Risk Response Strategy**

- Controls strengthening Incident Response Capabilities need to be implemented.
- Periodically reviewing the effectiveness of Security Controls can help strengthen the controls in place and reduce the probabilities of vulnerabilities.
- Intrusion Prevention Systems and regular update of digital signatures need to be done to proactively mitigate uprising threats.
- Patches need to be regularly checked, tested in an isolated environment and patched.
- Audit Trails control can be implemented and reviewed to identify potential service and process problems.
- Intermittently test the security configurations, backup the configurations and store them offline.
- Continually monitor and assess the security of management and critical systems, networks and infrastructure.
- Test backups of the system consistently and schedule operating system patches and hardware firmware patches at routine intervals.
- SIEM technology can be integrated to integrate multiple log formats from different sources and generate alerts on identified traffic patterns.
- By applying such various countermeasures, it is also necessary to test the incident response plan periodically to evaluate the effectiveness and update the plan accordingly.
- Monitor and log networking devices and verify their configurations schedule periodically.

- Manage and store the access information of networking devices by using Authentication, Authorization and Accounting services, to limit the access and only required privileges to the user.
- Document, review and update the Disaster recovery, Business continuity and continency plans.
- Reviewing and monitoring the log files of networking devices, can help in identifying potential exploitation attempts, to harden the networking devices
- Implement backup solutions to automatically back up critical data and keep the backup data in a secure and remotely isolated environment.
- Implement security checklist to audit and harden the application configurations and allow only the application modules and services that are required as per business needs.
- Implement Cross-Site Scripting and Cross-Site Scripting forgery protections to prevent from the most common attacks.
- Audit the code and services that are being provided by third-party while not being hosted on the server to ensure that there is no invalidated code being delivered.
- Blocking the most commonly exploited wireless attacks identified in this plan along with detection and reporting of any additional attacks can strengthen the prevention control capabilities.
- Generate automated event triggering, event log capturing and creation of customizable reports.
- Implementation of Wireless Intrusion Prevention/ Detection Systems to detect and classify various devices supporting 802.11 standards connected to wired and wireless networks.
- Implement MFA and EAP-TLS certificate or above based methods to ensure secure authentication for wireless transactions.

List of Cybersecurity Specialty Areas that exist in Symettrica

NICE Specialty Area
Risk Management (RSK)
Software Development (DEV)
Systems Architecture (ARC)
Data Administration (DTA)
Customer Service and Technical Support (STS)
Network Services (NET)
Cybersecurity Management (MGT)
Incident Response (CIR)
Vulnerability Assessment and Management (VAM)

List of Cybersecurity Work Roles that exist in your company

WORK ROLES
Authorizing Official/Designating Representative
Security Control Assessor
Software Developer
Secure Software Assessor
Enterprise Architect
Security Architect
Data Administrator
Data Analyst
Technical Support Specialist
Network Operations Specialist
Information Systems Security Manager
Communications Security (COMSEC) Manager
Cyber Defense Incident Responder
Vulnerability Assessment Analyst

List of Cybersecurity Tasks that exist in your company

Cybersecurity Tasks
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.
Establish acceptable limits for the software application, network, or system.
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.
Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).
Establish acceptable limits for the software application, network, or system.
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.
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
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).
Verify and update security documentation reflecting the application/system security design features.
Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
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.
Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.
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.

Identify basic common coding flaws at a high level.
Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development.
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.
Perform integrated quality assurance testing for security functionality and resiliency attack.
Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
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.
Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
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.
Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.
Identify and leverage the enterprise-wide version control system while designing and developing secure applications.
Consult with customers about software system design and maintenance.
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.
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.
Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.
Develop software system testing and validation procedures, programming, and documentation.
Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.
Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.
Determine and document software patches or the extent of releases that would leave software vulnerable.
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.
Consult with engineering staff to evaluate interface between hardware and software.
Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.
Identify basic common coding flaws at a high level.
Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development.
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.
Perform integrated quality assurance testing for security functionality and resiliency attack.
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
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.
Perform penetration testing as required for new or updated applications.
Consult with customers about software system design and maintenance.
Direct software programming and development of documentation.
Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.
Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.
Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.
Develop secure software testing and validation procedures.
Develop system testing and validation procedures, programming, and documentation.
Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.
Determine and document software patches or the extent of releases that would leave software vulnerable.
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.
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.
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.
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.
Develop enterprise architecture or system components required to meet user needs.
Document and update as necessary all definition and architecture activities.
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.
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.
Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
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).
Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
Analyze candidate architectures, allocate security services, and select security mechanisms.
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.
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.
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.
Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.
Translate proposed capabilities into technical requirements.
Assess and design security management functions as related to cyberspace.
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.
Manage the compilation, cataloging, caching, distribution, and retrieval of data.
Monitor and maintain databases to ensure optimal performance.
Perform backup and recovery of databases to ensure data integrity.
Provide recommendations on new database technologies and architectures.
Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.
Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.
Maintain assured message delivery systems.
Implement data management standards, requirements, and specifications.
Implement data mining and data warehousing applications.
Install and configure database management systems and software.
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.
Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.

Provide recommendations on new database technologies and architectures.
Analyze data sources to provide actionable recommendations.
Assess the validity of source data and subsequent findings.
Collect metrics and trending data.
Conduct hypothesis testing using statistical processes.
Confer with systems analysts, engineers, programmers, and others to design application.
Develop and facilitate data-gathering methods.
Develop strategic insights from large data sets.
Present technical information to technical and nontechnical audiences.
Present data in creative formats.
Program custom algorithms.
Provide actionable recommendations to critical stakeholders based on data analysis and findings.
Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.
Effectively allocate storage capacity in the design of data management systems.
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).
Utilize different programming languages to write code, open files, read files, and write output to different files.
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.
Maintain incident tracking and solution database.
Diagnose and resolve customer reported system incidents, problems, and events.
Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.
Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.
Administer accounts, network rights, and access to systems and equipment.
Perform asset management/inventory of information technology (IT) resources.
Monitor and report client-level computer system performance.
Develop a trend analysis and impact report.
Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
Develop and implement network backup and recovery procedures.
Diagnose network connectivity problem.
Implement new system design procedures, test procedures, and quality standards.

Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
Install or replace network hubs, routers, and switches.
Integrate new systems into existing network architecture.
Monitor network capacity and performance.
Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
Provide feedback on network requirements, including network architecture and infrastructure.
Test and maintain network infrastructure including software and hardware devices.
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.
Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.
Oversee the information security training and awareness program.
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.
Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.
Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.
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.
Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.
Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.
Recognize a possible security violation and take appropriate action to report the incident, as required.
Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.
Recommend policy and coordinate review and approval.
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).
Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.

Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.
Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
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.
Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).
Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.
Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.
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.
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.
Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
Ensure that security improvement actions are evaluated, validated, and implemented as required.
Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.
Evaluate cost/benefit, economic, and risk analysis in decision-making process.
Recognize a possible security violation and take appropriate action to report the incident, as required.
Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
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.
Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
Perform cyber defense trend analysis and reporting.
Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
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).
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.
Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).
Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.
Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.
Coordinate with intelligence analysts to correlate threat assessment data.
Write and publish after action reviews.
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.
Coordinate incident response functions.
Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
Conduct and/or support authorized penetration testing on enterprise network assets.
Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.
Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.
Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.
Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).
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).

Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).

Comparison of the NCWF recommended Cybersecurity Specialty Areas with your company's existing Cybersecurity Specialty Areas

NICE Specialty Area	IMPLEMENTATION STATUS
Risk Management (RSK)	PRESENT
Software Development (DEV)	PRESENT
Systems Architecture (ARC)	PRESENT
Technology R&D (TRD)	ABSENT
Systems Requirements Planning (SRP)	ABSENT
Test and Evaluation (TST)	ABSENT
Systems Development (SYS)	ABSENT
Data Administration (DTA)	PRESENT
Knowledge Management (KMG)	ABSENT
Customer Service and Technical Support (STS)	PRESENT
Network Services (NET)	PRESENT
Systems Administration (ADM)	ABSENT
Systems Analysis (ANA)	ABSENT
Legal Advice and Advocacy (LGA)	ABSENT
Training, Education, and Awareness (TEA)	ABSENT
Cybersecurity Management (MGT)	PRESENT
Strategic Planning and Policy (SPP)	ABSENT
Executive Cyber Leadership (EXL)	ABSENT
Program/Project Management (PMA) and Acquisition	ABSENT
Cybersecurity Defense Analysis (CDA)	ABSENT
Cybersecurity Defense Infrastructure Support (INF)	ABSENT
Incident Response (CIR)	PRESENT
Vulnerability Assessment and Management (VAM)	PRESENT
Threat Analysis (TWA)	ABSENT
Exploitation Analysis (EXP)	ABSENT
All-Source Analysis (ASA)	ABSENT
Targets (TGT)	ABSENT
Language Analysis (LNG)	ABSENT
Collection Operations (CLO)	ABSENT
Cyber Operational Planning (OPL)	ABSENT
Cyber Operations (OPS)	ABSENT
Cyber Investigation (INV)	ABSENT
Digital Forensics (FOR)	ABSENT

Comparison of the NCWF recommended Cybersecurity Work Roles with Symetrica's existing Cybersecurity Work Roles

AREA	WORK ROLES	STATUS
Risk Management (RSK)	Authorizing Official/Designating Representative	PRESENT
	Security Control Assessor	PRESENT
Software Development (DEV)	Software Developer	PRESENT
	Secure Software Assessor	PRESENT
Systems Architecture (ARC)	Enterprise Architect	PRESENT
	Security Architect	PRESENT
Technology R&D (TRD)	Research & Development Specialist	ABSENT
Systems Requirements Planning (SRP)	Systems Requirements Planner	ABSENT
Test and Evaluation (TST)	System Testing and Evaluation Specialist	ABSENT
Systems Development (SYS)	Information Systems Security Developer	ABSENT
	Systems Developer	ABSENT
Data Administration (DTA)	Database Administrator	PRESENT
	Data Analyst	PRESENT
Knowledge Management (KMG)	Knowledge Manager	ABSENT
Customer Service and Technical Support (STS)	Technical Support Specialist	PRESENT
Network Services (NET)	Network Operations Specialist	ABSENT
Systems Administration (ADM)	System Administrator	ABSENT
Systems Analysis (ANA)	Systems Security Analyst	ABSENT

Legal Advice and Advocacy (LGA)	Database Administrator	ABSENT
	Data Analyst	ABSENT
Training, Education, and Awareness (TEA)	Knowledge Manager	ABSENT
	Technical Support Specialist	ABSENT
Cybersecurity Management (MGT)	Network Operations Specialist	PRESENT
	System Administrator	ABSENT
Strategic Planning and Policy (SPP)	Systems Security Analyst	ABSENT
	Cyber Legal Advisor	ABSENT
Executive Cyber Leadership (EXL)	Privacy Officer/Privacy Compliance Manager	ABSENT
Program/Project Management (PMA) and Acquisition	Program Manager	ABSENT
	IT Project Manager	ABSENT
	Product Support Manager	ABSENT
	IT Investment/Portfolio Manager	ABSENT
	IT Program Auditor	ABSENT
Cybersecurity Defense Analysis (CDA)	Cyber Defense Analyst	ABSENT
Cybersecurity Defense Infrastructure Support (INF)	Cyber Defense Infrastructure Support Specialist	ABSENT
Incident Response (CIR)	Cyber Defense Incident Responder	PRESENT
Vulnerability Assessment and Management (VAM)	Vulnerability Assessment Analyst	PRESENT
Threat Analysis (TWA)	Threat/Warning Analyst	ABSENT
Exploitation Analysis (EXP)	Exploitation Analyst	ABSENT
All-Source Analysis (ASA)	All-Source Analyst	ABSENT
	Mission Assessment Specialist	ABSENT
Targets (TGT)	Target Developer	ABSENT
	Target Network Analyst	ABSENT
Language Analysis (LNG)	Multi-Disciplined Language Analyst	ABSENT

Collection Operations (CLO)	All Source-Collection Manager	ABSENT
	All Source-Collection Requirements Manager	ABSENT
Cyber Operational Planning (OPL)	Cyber Intel Planner	ABSENT
	Cyber Ops Planner	ABSENT
	Partner Integration Planner	ABSENT
Cyber Operations (OPS)	Cyber Operator	ABSENT
Cyber Investigation (INV)	Cyber Crime Investigator	ABSENT
Digital Forensics (FOR)	Law Enforcement /CounterIntelligence Forensics Analyst	ABSENT
	Cyber Defense Forensics Analyst	PRESENT

Comparison the NCWF recommended Cybersecurity Tasks with Symetrica's existing Cybersecurity Tasks

WORK ROLE	TASK	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).	PRESENT
	Establish acceptable limits for the software application, network, or system.	PRESENT

	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	ABSENT
	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).	PRESENT
	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.	PRESENT
	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.	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
	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	PRESENT
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	ABSENT
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	PRESENT
	Assess the effectiveness of security controls.	ABSENT
	Assess all the configuration management (change configuration/release management) processes.	PRESENT
Software Developer	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.	PRESENT
	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.	PRESENT
	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.	PRESENT
	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.	PRESENT
	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.	PRESENT
	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.	ABSENT
	Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	ABSENT
	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.	PRESENT
	Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.	PRESENT
	Develop software system testing and validation procedures, programming, and documentation.	PRESENT
	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.	PRESENT

	Determine and document software patches or the extent of releases that would leave software vulnerable.	ABSENT
Secure Software Assessor	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	ABSENT
	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.	ABSENT
	Develop threat model based on customer interviews and requirements.	ABSENT
	Consult with engineering staff to evaluate interface between hardware and software.	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.	PRESENT
	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.	PRESENT
	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.	PRESENT
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	PRESENT
	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.	PRESENT
	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.	ABSENT
	Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.	PRESENT
	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.	PRESENT
	Develop secure software testing and validation procedures.	PRESENT
	Develop system testing and validation procedures, programming, and documentation.	ABSENT
	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.	ABSENT
	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.	ABSENT
	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).	ABSENT
	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.	PRESENT

	Write detailed functional specifications that document the architecture development process.	ABSENT
	Analyze user needs and requirements to plan architecture.	ABSENT
	Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	ABSENT
	Develop enterprise architecture or system components required to meet user needs.	ABSENT
	Document and update as necessary all definition and architecture activities.	PRESENT
	Integrate results regarding the identification of gaps in security architecture.	PRESENT
	Plan implementation strategy to ensure that enterprise components can be integrated and aligned.	ABSENT
	Translate proposed capabilities into technical requirements.	ABSENT
	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.	ABSENT
	Integrate key management functions as related to cyberspace.	ABSENT
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.	ABSENT
	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.	PRESENT
	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.	PRESENT
	Provide advice on project costs, design concepts, or design changes.	ABSENT

	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).	ABSENT
	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	PRESENT
	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.	PRESENT
	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.	PRESENT
	Write detailed functional specifications that document the architecture development process.	ABSENT
	Analyze user needs and requirements to plan architecture.	ABSENT
	Develop enterprise architecture or system components required to meet user needs.	ABSENT
	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.	PRESENT
	Assess and design security management functions as related to cyberspace.	ABSENT
Research and Development Specialist	Review and validate data mining and data warehousing programs, processes, and requirements.	ABSENT
	Research current technology to understand capabilities of required system or network.	ABSENT
	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.	ABSENT
	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.	ABSENT
Systems Requirements Planner (SP-SRP-001):	Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.	PRESENT
	Consult with customers to evaluate functional requirements.	PRESENT
	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.	PRESENT
	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.	PRESENT
	Develop and document User Experience (UX) requirements including information architecture and user interface requirements.	PRESENT
	Design and document quality standards.	PRESENT
	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.	PRESENT
	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
Systems Requirements Planner (SP-SRP-001):	Determine level of assurance of developed capabilities based on test results.	PRESENT
	Develop test plans to address specifications and requirements.	ABSENT
	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	PRESENT
	Make recommendations based on test results.	ABSENT
	Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.	ABSENT
	Create auditable evidence of security measures.	PRESENT
	Validate specifications and requirements for testability.	
	Analyze the results of software, hardware, or interoperability testing.	PRESENT
	Perform developmental testing on systems under development.	ABSENT
	Perform interoperability testing on systems exchanging electronic information with other systems.	ABSENT
	Perform operational testing.	ABSENT
	Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.	PRESENT
	Record and manage test data.	ABSENT
System Test & Evaluation Specialist (SP-TST-001):	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.	ABSENT
	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.	PRESENT
	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).	PRESENT
	Design and develop cybersecurity or cybersecurity-enabled products.	PRESENT
	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.	PRESENT
	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.	ABSENT
	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.	PRESENT
	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.	PRESENT
	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.	PRESENT
	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.	PRESENT
	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.	ABSENT
	Utilize models and simulations to analyze or predict system performance under different operating conditions.	ABSENT
	Design and develop key management functions (as related to cybersecurity).	ABSENT

	Analyze user needs and requirements to plan and conduct system security development.	PRESENT
Information Systems Security Developer (SP-SYS-001):	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).	PRESENT
	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.	PRESENT
	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.	PRESENT
	Design to security requirements to ensure requirements are met for all systems and/or applications.	ABSENT
	Develop mitigation strategies to address cost, schedule, performance, and security risks.	ABSENT
	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.	PRESENT
	Trace system requirements to design components and perform gap analysis.	PRESENT
	Verify stability, interoperability, portability, and/or scalability of system architecture.	ABSENT
Systems Developer (SP-SYS-002):	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.	ABSENT
	Design and develop cybersecurity or cybersecurity-enabled products.	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.	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.	PRESENT
	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.	PRESENT
	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.	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.	PRESENT
	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.	PRESENT
	Design and develop system administration and management functionality for privileged access users.	PRESENT
	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).	PRESENT

	Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.	PRESENT
	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.	PRESENT
	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	PRESENT
	Provide support to test and evaluation activities.	ABSENT
	Trace system requirements to design components and perform gap analysis.	ABSENT
	Verify stability, interoperability, portability, and/or scalability of system architecture.	ABSENT
	Analyze user needs and requirements to plan and conduct system development.	ABSENT
	Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.	PRESENT
	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
	Analyze and plan for anticipated changes in data capacity requirements.	ABSENT
	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.	ABSENT
	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.	PRESENT
	Perform backup and recovery of databases to ensure data integrity.	ABSENT
	Provide recommendations on new database technologies and architectures.	PRESENT
	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.	ABSENT
	Implement data management standards, requirements, and specifications.	PRESENT
	Implement data mining and data warehousing applications.	ABSENT
	Install and configure database management systems and software.	ABSENT
Database Administrator (OM-DTA-001):	Analyze and define data requirements and specifications.	PRESENT
	Analyze and plan for anticipated changes in data capacity requirements.	ABSENT
	Develop data standards, policies, and procedures.	ABSENT
	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.	PRESENT
	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.	PRESENT
	Develop and facilitate data-gathering methods.	ABSENT
	Develop strategic insights from large data sets.	ABSENT
	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.	PRESENT
	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
	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.	PRESENT
	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).	ABSENT
	Develop and implement data mining and data warehousing programs.	ABSENT
Data Analyst (OM-DTA-002):	Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.	PRESENT
	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.	PRESENT
	Lead efforts to promote the organization's use of knowledge management and information sharing.	PRESENT
	Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).	PRESENT
	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 (OM-STS-001):	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.	
	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.	PRESENT

	Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.	ABSENT
	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.	ABSENT
Network Operations Specialist	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	ABSENT
	Troubleshoot system hardware and software.	ABSENT
	Analyze incident data for emerging trends.	PRESENT
	Develop and deliver technical training to educate others or meet customer needs.	ABSENT
	Troubleshoot hardware/software interface and interoperability problems.	PRESENT
System Administrator	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	ABSENT
	Review, conduct, or participate in audits of cyber programs and projects.	PRESENT
	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).	PRESENT
	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).	PRESENT
	Support the CIO in the formulation of cyber-related policies.	ABSENT
	Provide support to test and evaluation activities.	ABSENT
	Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.	PRESENT
Vulnerability Assessment Analyst	Record and manage test data.	ABSENT
	Trace system requirements to design components and perform gap analysis.	PRESENT
	Translate proposed capabilities into technical requirements.	ABSENT
	Verify stability, interoperability, portability, and/or scalability of system architecture.	ABSENT
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	ABSENT

	Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.	PRESENT
	Research and evaluate available technologies and standards to meet customer requirements.	PRESENT
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	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).	PRESENT
	Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).	PRESENT
	Draft and publish supply chain security and risk management documents.	ABSENT
	Review and approve a supply chain security/risk management policy.	ABSENT
	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	PRESENT
	Determine and document software patches or the extent of releases that would leave software vulnerable.	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.	ABSENT
	Assess and design security management functions as related to cyberspace.	ABSENT
	Integrate key management functions as related to cyberspace.	ABSENT
	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.	PRESENT
	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
	Accurately characterize targets.	ABSENT
	Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements.	PRESENT
	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.	PRESENT

	Analyze feedback to determine extent to which collection products and services are meeting requirements.	ABSENT
	Analyze incoming collection requests.	PRESENT
	Analyze internal operational architecture, tools, and procedures for ways to improve performance.	ABSENT
	Analyze target operational architecture for ways to gain access.	PRESENT
	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements).	ABSENT
	Answer requests for information.	ABSENT
	Apply and utilize authorized cyber capabilities to enable access to targeted networks.	PRESENT
	Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.	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
	Assess and apply operational environment factors and risks to collection management process.	PRESENT
	Apply and obey applicable statutes, laws, regulations and policies.	ABSENT
	Coordinate for intelligence support to operational planning activities.	ABSENT
	Assess all-source intelligence and recommend targets to support cyber operation objectives.	ABSENT
	Assess efficiency of existing information exchange and management systems.	PRESENT
	Assess performance of collection assets against prescribed specifications.	ABSENT
	Assess target vulnerabilities and/or operational capabilities to determine course of action.	ABSENT
	Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and adjust collection strategies and collection requirements accordingly.	PRESENT
	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	PRESENT
	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.	PRESENT
Systems Security Analyst	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
	Assist in the development and refinement of priority information requirements.	ABSENT
	Provide expertise to the development of measures of effectiveness and measures of performance.	PRESENT
	Assist in the identification of intelligence collection shortfalls.	ABSENT
	Enable synchronization of intelligence support plans across partner organizations as required.	ABSENT
	Perform analysis for target infrastructure exploitation activities.	ABSENT
	Provide input to the identification of cyber-related success criteria.	PRESENT
	Brief threat and/or target current situations.	ABSENT
Cyber Legal Advisor	Build and maintain electronic target folders.	ABSENT
	Classify documents in accordance with classification guidelines.	ABSENT
	Close requests for information once satisfied.	ABSENT
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	ABSENT
	Collaborate with development organizations to create and deploy the tools needed to achieve objectives.	PRESENT
	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	ABSENT
	Collaborate with other internal and external partner organizations on target access and operational issues.	PRESENT
	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).	ABSENT
	Collaborate with customer to define information requirements.	ABSENT
	Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.	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
	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	PRESENT
	Identify and conduct analysis of target communications to identify information essential to support operations.	PRESENT
	Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.	ABSENT
	Conduct access enabling of wireless computer and digital networks.	ABSENT
	Conduct collection and processing of wireless computer and digital networks.	PRESENT

	Conduct end-of-operations assessments.	ABSENT
	Conduct exploitation of wireless computer and digital networks.	ABSENT
	Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.	ABSENT
	Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.	PRESENT
	Conduct in-depth research and analysis.	ABSENT
	Conduct network scouting and vulnerability analyses of systems within a network.	ABSENT
	Conduct nodal analysis.	PRESENT
	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.	PRESENT
	Conduct quality control to determine validity and relevance of information gathered about networks.	ABSENT
Privacy Officer/Privacy Compliance Manager	Develop, review and implement all levels of planning guidance in support of cyber operations.	ABSENT
	Conduct survey of computer and digital networks.	PRESENT
	Conduct target research and analysis.	
	Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.	PRESENT
	Construct collection plans and matrixes using established guidance and procedures.	ABSENT
	Contribute to crisis action planning for cyber operations.	PRESENT
	Contribute to the development of the organization's decision support tools if necessary.	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
	Incorporate intelligence equities into the overall design of cyber operations plans.	PRESENT
	Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.	PRESENT
	Coordinate inclusion of collection plan in appropriate documentation.	ABSENT
	Coordinate target vetting with appropriate partners.	ABSENT
	Re-task or re-direct collection assets and resources.	ABSENT
	Coordinate with intelligence and cyber defense partners to obtain relevant essential information.	PRESENT

	Coordinate with intelligence planners to ensure that collection managers receive information requirements.	PRESENT
	Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks.	PRESENT
	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
Program Manager	Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities.	PRESENT
	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	PRESENT
	Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).	PRESENT
	Detect exploits against targeted networks and hosts and react accordingly.	ABSENT
	Determine course of action for addressing changes to objectives, guidance, and operational environment.	PRESENT
	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.	ABSENT
	Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.	ABSENT
	Determine organizations and/or echelons with collection authority over all accessible collection assets.	PRESENT
	Determine what technologies are used by a given target.	ABSENT
	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	ABSENT
	Develop all-source intelligence targeting materials.	ABSENT
	Apply analytic techniques to gain more target information.	ABSENT
	Develop and maintain deliberate and/or crisis plans.	ABSENT
	Develop and review specific cyber operations guidance for integration into broader planning activities.	PRESENT
	Develop and review intelligence guidance for integration into supporting cyber operations planning and execution.	PRESENT
	Develop coordinating instructions by collection discipline for each phase of an operation.	ABSENT
	Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives.	PRESENT
	Develop detailed intelligence support to cyber operations requirements.	ABSENT
	Develop information requirements necessary for answering priority information requests.	PRESENT

	Develop measures of effectiveness and measures of performance.	ABSENT
	Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis.	ABSENT
	Develop munitions effectiveness assessment or operational assessment materials.	PRESENT
	Develop new techniques for gaining and keeping access to target systems.	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.	PRESENT
	Develop potential courses of action.	ABSENT
	Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.	ABSENT
	Develop strategy and processes for partner planning, operations, and capability development.	PRESENT
	Develop, implement, and recommend changes to appropriate planning procedures and policies.	ABSENT
	Develop, maintain, and assess cyber cooperation security agreements with external partners.	ABSENT
	Devise, document, and validate cyber operation strategy and planning documents.	ABSENT
IT Project Manager	Disseminate reports to inform decision makers on collection issues.	PRESENT
	Disseminate tasking messages and collection plans.	ABSENT
	Conduct and document an assessment of the collection results using established procedures.	ABSENT
	Draft cyber intelligence collection and production requirements.	PRESENT
	Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.	PRESENT
	Engage customers to understand customers’ intelligence needs and wants.	PRESENT
	Ensure operational planning efforts are effectively transitioned to current operations.	PRESENT
	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	PRESENT
	Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems.	ABSENT
	Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.	PRESENT

	Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures.	PRESENT
	Estimate operational effects generated through cyber activities.	ABSENT
	Evaluate threat decision-making processes.	ABSENT
	Identify threat vulnerabilities.	ABSENT
	Identify threats to Blue Force vulnerabilities.	PRESENT
	Evaluate available capabilities against desired effects to recommend efficient solutions.	PRESENT
	Evaluate extent to which collected information and/or produced intelligence satisfy information requests.	ABSENT
	Evaluate intelligence estimates to support the planning cycle.	PRESENT
	Evaluate the conditions that affect employment of available cyber intelligence capabilities.	PRESENT
	Generate and evaluate the effectiveness of network analysis strategies.	ABSENT
	Evaluate extent to which collection operations are synchronized with operational requirements.	ABSENT
	Evaluate the effectiveness of collection operations against the collection plan.	PRESENT
	Examine intercept-related metadata and content with an understanding of targeting significance.	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
	Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.	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
	Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.	PRESENT
	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.	PRESENT
	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.	PRESENT
	Incorporate intelligence and counterintelligence to support plan development.	ABSENT

	Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)	PRESENT
	Generate requests for information.	PRESENT
	Identify threat tactics, and methodologies.	ABSENT
	Identify all available partner intelligence capabilities and limitations supporting cyber operations.	ABSENT
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	PRESENT
	Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.	ABSENT
	Identify and manage security cooperation priorities with external partners.	PRESENT
	Identify and submit intelligence requirements for the purposes of designating priority information requirements.	ABSENT
	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	ABSENT
	Identify collection gaps and potential collection strategies against targets.	PRESENT
	Identify coordination requirements and procedures with designated collection authorities.	ABSENT
	Identify critical target elements.	ABSENT
	Identify intelligence gaps and shortfalls.	PRESENT
	Identify cyber intelligence gaps and shortfalls for cyber operational planning.	ABSENT
Product Support Manager	Identify gaps in our understanding of target technology and developing innovative collection approaches.	PRESENT
	Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.	ABSENT
	Identify network components and their functionality to enable analysis and target development.	PRESENT
	Identify potential collection disciplines for application against priority information requirements.	ABSENT
	Identify potential points of strength and vulnerability within a network.	PRESENT
	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	ABSENT
	Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.	PRESENT
	Identify, locate, and track targets via geospatial analysis techniques.	ABSENT
	Provide input to or develop courses of action based on threat factors.	ABSENT

	Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.	ABSENT
	Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.	PRESENT
	Initiate requests to guide tasking and assist with collection management.	ABSENT
	Integrate cyber planning/targeting efforts with other organizations.	ABSENT
	Interpret environment preparations assessments to determine a course of action.	PRESENT
	Issue requests for information.	ABSENT
	Lead and coordinate intelligence support to operational planning.	ABSENT
	Lead or enable exploitation operations in support of organization objectives and target requirements.	PRESENT
	Link priority collection requirements to optimal assets and resources.	ABSENT
	Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.	ABSENT
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	PRESENT
	Maintain situational awareness and functionality of organic operational infrastructure.	ABSENT
	Maintain situational awareness of cyber-related intelligence requirements and associated tasking.	ABSENT
	Maintain situational awareness of partner capabilities and activities.	PRESENT
	Maintain situational awareness to determine if changes to the operating environment require review of the plan.	ABSENT
	Maintain target lists (i.e., RTL, JTL, CTL, etc.).	ABSENT
	Make recommendations to guide collection in support of customer requirements.	ABSENT
	Modify collection requirements as necessary.	PRESENT
	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	PRESENT
	Monitor and report on validated threat activities.	ABSENT
	Monitor completion of reallocated collection efforts.	PRESENT
	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
	Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.	PRESENT
	Monitor target networks to provide indications and warning of target communications changes or processing failures.	ABSENT
	Monitor the operational environment for potential factors and risks to the collection operation management process.	PRESENT
IT Investment/Portfolio Manager	Operate and maintain automated systems for gaining and maintaining access to target systems.	ABSENT
	Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence 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
	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	PRESENT
	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	ABSENT
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	PRESENT
	WITHDRAWN: Provide subject matter expertise in course of action development.	ABSENT
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	PRESENT
	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	PRESENT
	Provide subject matter expertise to development of exercises.	ABSENT
	Propose policy which governs interactions with external coordination groups.	ABSENT
	Perform content and/or metadata analysis to meet organization objectives.	PRESENT
	Conduct cyber activities to degrade/remove information resident in computers and computer networks.	ABSENT
	Perform targeting automation activities.	PRESENT
	Characterize websites.	PRESENT
	Provide subject matter expertise to website characterizations.	PRESENT
	Prepare for and provide subject matter expertise to exercises.	PRESENT
	Prioritize collection requirements for collection platforms based on platform capabilities.	ABSENT
	Process exfiltrated data for analysis and/or dissemination to customers.	PRESENT

	Produce network reconstructions.	ABSENT
	Produce target system analysis products.	PRESENT
	Profile network or system administrators and their activities.	
	Profile targets and their activities.	PRESENT
	Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.	ABSENT
	Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.	PRESENT
	Provide aim point and reengagement recommendations.	ABSENT
	Provide analyses and support for effectiveness assessment.	ABSENT
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	PRESENT
	Provide cyber focused guidance and advice on intelligence support plan inputs.	ABSENT
	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	PRESENT
	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 for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	ABSENT
	Provide input and assist in post-action effectiveness assessments.	PRESENT
	Provide input and assist in the development of plans and guidance.	ABSENT
	Provide input for targeting effectiveness assessments for leadership acceptance.	ABSENT
	Provide input to the administrative and logistical elements of an operational support plan.	PRESENT
	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	ABSENT
	Provide effectiveness support to designated exercises, and/or time sensitive operations.	ABSENT
	Provide operations and reengagement recommendations.	ABSENT
	Provide planning support between internal and external partners.	PRESENT
	Provide real-time actionable geolocation information.	PRESENT
	Provide target recommendations which meet leadership objectives.	ABSENT
	Provide targeting products and targeting support as designated.	ABSENT
	Provide time sensitive targeting support.	PRESENT

	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	ABSENT
IT Program Auditor	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	PRESENT
	Review appropriate information sources to determine validity and relevance of information gathered.	ABSENT
	Reconstruct networks in diagram or report format.	ABSENT
	Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.	ABSENT
	Report intelligence-derived significant network events and intrusions.	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.	PRESENT
	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.	ABSENT
	Review and comprehend organizational leadership objectives and guidance for planning.	PRESENT
	Review capabilities of allocated collection assets.	PRESENT
	Review intelligence collection guidance for accuracy/applicability.	ABSENT
	Review list of prioritized collection requirements and essential information.	PRESENT
	Review and update overarching collection plan, as required.	PRESENT
	Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.	ABSENT
	Revise collection matrix based on availability of optimal assets and resources.	ABSENT
Cyber Defense Analyst	Sanitize and minimize information to protect sources and methods.	PRESENT
	Scope the cyber intelligence planning effort.	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.	PRESENT
	Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.	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.	ABSENT
	Submit information requests to collection requirement management section for processing as collection requests.	PRESENT
	Submit or respond to requests for deconfliction of cyber operations.	ABSENT
	Support identification and documentation of collateral effects.	ABSENT
	Synchronize cyber international engagement activities and associated resource requirements as appropriate.	ABSENT
	Synchronize cyber portions of security cooperation plans.	PRESENT
	Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.	ABSENT
Cyber Defense Infrastructure Support Specialist	Test and evaluate locally developed tools for operational use.	PRESENT
	Test internal developed tools and techniques against target tools.	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.	PRESENT
	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.	PRESENT
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	ABSENT
	Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.	PRESENT
	Document lessons learned that convey the results of events and/or exercises.	ABSENT
	Advise managers and operators on language and cultural issues that impact organization objectives.	PRESENT
	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.	PRESENT
	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.	PRESENT

	Perform quality review and provide feedback on transcribed or translated materials.	PRESENT
	Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.	PRESENT
	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.	PRESENT
	Provide feedback to collection managers to enhance future collection and analysis.	PRESENT
	Perform foreign language and dialect identification in initial source data.	ABSENT
	Perform or support technical network analysis and mapping.	PRESENT
	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.	PRESENT
	Tip critical or time-sensitive information to appropriate customers.	PRESENT
	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).	PRESENT
	Provide near-real time language analysis support (e.g., live operations).	ABSENT
	Identify cyber/technology-related terminology in the target language.	PRESENT
	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.	PRESENT
	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.	ABSENT
	Liaise with regulatory and accrediting bodies.	ABSENT

	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.	ABSENT
	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.	PRESENT
	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.	PRESENT
	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	ABSENT
	Serve in a leadership role for Privacy Oversight Committee activities	PRESENT
Cyber Defense Incident Responder	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	PRESENT
	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	PRESENT
	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	PRESENTS
	Serve as the information privacy liaison for users of technology systems	ABSENT
	Act as a liaison to the information systems department	PRESENT
Threat/Warning Analyst	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	
	Conduct on-going privacy training and awareness activities	PRESENT

	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.	PRESENT
	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	PRESENT
Source-Collection Manager	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	PRESENT
	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	PRESENT
	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.	PRESENT
	Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations	PRESENT
	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	PRESENT
	Provide leadership in the planning, design and evaluation of privacy and security related projects	PRESENT

	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	PRESENT
	Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information	PRESENT
	Monitor systems development and operations for security and privacy compliance	ABSENT
All Source-Collection Requirements Manager	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	PRESENT
	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	PRESENT
	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	PRESENT
	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	PRESENT
	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	PRESENT
	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	PRESENT
	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	PRESENT

	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	PRESENT
	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	ABSENT
	Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials	PRESENT
	Develop and maintain appropriate communications and training to promote and educate all workforce members and members of the Board regarding privacy compliance issues and requirements, and the consequences of noncompliance	ABSENT
	Determine business partner requirements related to the organization's privacy program.	PRESENT
	Establish and administer a process for receiving, documenting, tracking, investigating and taking corrective action as appropriate on complaints concerning the company's privacy policies and procedures.	PRESENT
	Cooperate with the relevant regulatory agencies and other legal entities, and organization officers, in any compliance reviews or investigations.	PRESENT
	Perform ongoing privacy compliance monitoring activities.	ABSENT
	Monitor advancements in information privacy technologies to ensure organization adoption and compliance.	PRESENT
	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 Intel Planner	Appoint and guide a team of IT security experts.	PRESENT
	Collaborate with key stakeholders to establish a cybersecurity risk management program.	ABSENT
	Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.	ABSENT
	Establish a risk management strategy for the organization that includes a determination of risk tolerance.	PRESENT
	Identify the missions, business functions, and mission/business processes the system will support.	PRESENT
	Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.	ABSENT
	Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.	ABSENT

	Identify stakeholder assets that require protection.	ABSENT
	Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.	ABSENT
	Define the stakeholder protection needs and stakeholder security requirements.	ABSENT
	Determine the placement of a system within the enterprise architecture.	ABSENT
	Identify organization-wide common controls that are available for inheritance by organizational systems.	PRESENT
	Conduct a second-level security categorization for organizational systems with the same impact level.	PRESENT
	Determine the boundary of a system.	ABSENT
	Identify the security requirements allocated to a system and to the organization.	ABSENT
	Identify the types of information to be processed, stored, or transmitted by a system.	ABSENT
	Categorize the system and document the security categorization results as part of system requirements.	PRESENT
	Describe the characteristics of a system.	
	Register the system with appropriate organizational program/management offices.	PRESENT
	Select the security controls for a system and document the functional description of the planned control implementations in a security plan.	
	Develop a strategy for monitoring security control effectiveness; coordinate the system-level strategy with the organization and mission/business process-level monitoring strategy.	PRESENT
Cyber Ops Planner	Review and approve security plans.	ABSENT
	Implement the security controls specified in a security plan or other system documentation.	ABSENT
	Document changes to planned security control implementation and establish the configuration baseline for a system.	ABSENT
	Develop, review, and approve a plan to assess the security controls in a system and the organization.	PRESENT
	Assess the security controls in accordance with the assessment procedures defined in a security assessment plan.	PRESENT
	Prepare a security assessment report documenting the issues, findings, and recommendations from the security control assessment.	ABSENT
	Conduct initial remediation actions on security controls based on the findings and recommendations of a security assessment report; reassess remediated controls.	PRESENT
	Prepare a plan of action and milestones based on the findings and recommendations of a security assessment report excluding any remediation actions taken.	ABSENT

	Assemble an authorization package and submit the package to an authorizing official for adjudication.	PRESENT
	Determine the risk from the operation or use of a system or the provision or use of common controls.	ABSENT
	Identify and implement a preferred course of action in response to the risk determined.	PRESENT
	Determine if the risk from the operation or use of the system or the provision or use of common controls, is acceptable.	ABSENT
	Monitor changes to a system and its environment of operation.	ABSENT
	Assess the security controls employed within and inherited by the system in accordance with an organization-defined monitoring strategy.	PRESENT
	Respond to risk based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in a plan of action and milestones.	ABSENT
	Update a security plan, security assessment report, and plan of action and milestones based on the results of a continuous monitoring process.	PRESENT
	Report the security status of a system (including the effectiveness of security controls) to an authorizing official on an ongoing basis in accordance with the monitoring strategy.	ABSENT
	Review the security status of a system (including the effectiveness of security controls) on an ongoing basis to determine whether the risk remains acceptable.	ABSENT
	Implement a system disposal strategy which executes required actions when a system is removed from service.	PRESENT
	Sponsor and promote continuous monitoring within the organization.	ABSENT
	Assign staff as needed to appropriate continuous monitoring working groups.	ABSENT
	Identify reporting requirements to support continuous monitoring activities.	PRESENT
	Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.	ABSENT
	Determine how to integrate a continuous monitoring program into the organization’s broader information security governance structures and policies.	PRESENT
	Use continuous monitoring scoring and grading metrics to make information security investment decisions to address persistent issues.	ABSENT
	Ensure that the continuous monitoring staff have the training and resources (e.g., staff and budget) needed to perform assigned duties.	PRESENT
	Work with organizational risk analysts to ensure that continuous monitoring reporting covers appropriate levels of the organization.	ABSENT

	Work with the organizational risk analysts to ensure risk metrics are defining realistically to support continuous monitoring.	ABSENT
	Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.	PRESENT
Partner Integration Planner	Establish triggers for unacceptable risk thresholds for continuous monitoring data.	ABSENT
	Work with organizational officials to establish system level reporting categories that can be used by the organization’s continuous monitoring program.	PRESENT
	Designate a qualified person to be responsible for the management and implementation of the continuous monitoring program.	ABSENT
	Identify the continuous monitoring stakeholders and establish a process to keep them informed about the program.	PRESENT
	Identify security oriented organization reporting requirements that are fulfilled by the continuous monitoring program.	ABSENT
	Use the continuous monitoring data to make information security investment decisions to address persistent issues.	PRESENT
	Define triggers within the continuous monitoring program that can be used to define unacceptable risk and result in action being taken to resolve.	ABSENT
	Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.	PRESENT
	Work with security managers to establish appropriate continuous monitoring reporting requirements at the system level.	ABSENT
	Use the continuous monitoring tools and technologies to assess risk on an ongoing basis.	PRESENT
	Establish appropriate reporting requirements in adherence to the criteria identified in the continuous monitoring program for use in automated control assessment.	ABSENT
	Use non-automated assessment methods where the data from the continuous monitoring tools and technologies is not yet of adequate sufficiency or quality.	PRESENT
	Develop processes with the external audit group on how to share information regarding the continuous monitoring program and its impact on security control assessment.	PRESENT
	Identify reporting requirements for use in automated control assessment to support continuous monitoring.	ABSENT
	Determine how the continuous monitoring results will be used in ongoing authorization.	PRESENT
	Establish continuous monitoring tools and technologies access control process and procedures.	ABSENT
	Ensure that continuous monitoring tools and technologies access control is managed adequately.	ABSENT
	Establish a process to provide technical help to continuous monitoring mitigators.	PRESENT

	Coordinate continuous monitoring reporting requirements across various users.	ABSENT
	Establish responsibilities for supporting implementation of each continuous monitoring tool or technology.	PRESENT
	Establish liaison with scoring and metrics working group to support continuous monitoring.	ABSENT
	Establish and operate a process to manage introduction of new risk to support continuous monitoring.	PRESENT
	Establish continuous monitoring configuration settings issues and coordination sub-group.	ABSENT
	Establish continuous monitoring tools and technologies performance measurement/management requirements.	PRESENT
	Using scores and grades to motivate and assess performance while addressing concerns to support continuous monitoring	ABSENT
	Work with security managers (i.e., system owners, information system security managers, information system security officers, etc.) to establish appropriate reporting requirements for continuous monitoring at the system level.	PRESENT
	Use continuous monitoring tools to assess risk on an ongoing basis.	ABSENT
	Use the continuous monitoring data to make information security investment decisions to address persistent issues.	PRESENT
	Respond to issues flagged during continuous monitoring, escalate and coordinate a response.	ABSENT
	Review findings from the continuous monitoring program and mitigate risks on a timely basis.	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
	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	PRESENT
	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	ABSENT
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	PRESENT
	WITHDRAWN: Provide subject matter expertise in course of action development.	ABSENT
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	PRESENT
	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	ABSENT
	Provide subject matter expertise to development of exercises.	PRESENT
	Propose policy which governs interactions with external coordination groups.	ABSENT

	Perform content and/or metadata analysis to meet organization objectives.	PRESENT
	Conduct cyber activities to degrade/remove information resident in computers and computer networks.	ABSENT
	Perform targeting automation activities.	ABSENT
	Characterize websites.	ABSENT
	Provide subject matter expertise to website characterizations.	PRESENT
	Prepare for and provide subject matter expertise to exercises.	ABSENT
	Prioritize collection requirements for collection platforms based on platform capabilities.	ABSENT
	Process exfiltrated data for analysis and/or dissemination to customers.	PRESENT
	Produce network reconstructions.	ABSENT
	Produce target system analysis products.	ABSENT
	Profile network or system administrators and their activities.	ABSENT
	Profile targets and their activities.	ABSENT
	Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.	PRESENT
Cyber Operator	Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.	PRESENT
	Provide aim point and reengagement recommendations.	ABSENT
	Provide analyses and support for effectiveness assessment.	
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	PRESENT
	Provide cyber focused guidance and advice on intelligence support plan inputs.	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.	PRESENT
	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	PRESENT
	Provide input and assist in post-action effectiveness assessments.	PRESENT
	Provide input and assist in the development of plans and guidance.	ABSENT
	Provide input for targeting effectiveness assessments for leadership acceptance.	PRESENT
	Provide input to the administrative and logistical elements of an operational support plan.	ABSENT

	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	PRESENT
	Provide effectiveness support to designated exercises, and/or time sensitive operations.	ABSENT
	Provide operations and reengagement recommendations.	PRESENT
	Provide planning support between internal and external partners.	ABSENT
	Provide real-time actionable geolocation information.	PRESENT
	Provide target recommendations which meet leadership objectives.	ABSENT
	Provide targeting products and targeting support as designated.	PRESENT
	Provide time sensitive targeting support.	ABSENT
	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	ABSENT
Cyber Crime Investigator Law Enforcement /Counterintelligence Forensics Analyst	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	PRESENT
	Review appropriate information sources to determine validity and relevance of information gathered.	ABSENT
	Reconstruct networks in diagram or report format.	ABSENT
	Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.	PRESENT
	Report intelligence-derived significant network events and intrusions.	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.	PRESENT
	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.	PRESENT
	Review and comprehend organizational leadership objectives and guidance for planning.	ABSENT
	Review capabilities of allocated collection assets.	PRESENT
	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.	PRESENT
	Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.	PRESENT
	Revise collection matrix based on availability of optimal assets and resources.	ABSENT
Cyber Defense Forensics Analyst	Sanitize and minimize information to protect sources and methods.	ABSENT

	Scope the cyber intelligence planning effort.	PRESENT
	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.	PRESENT
	Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.	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.	ABSENT
	Submit information requests to collection requirement management section for processing as collection requests.	PRESENT
	Submit or respond to requests for deconfliction of cyber operations.	ABSENT
	Support identification and documentation of collateral effects.	PRESENT
	Synchronize cyber international engagement activities and associated resource requirements as appropriate.	ABSENT
	Synchronize cyber portions of security cooperation plans.	ABSENT
	Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.	PRESENT
Exploitation Analyst	Test and evaluate locally developed tools for operational use.	ABSENT
	Test internal developed tools and techniques against target tools.	PRESENT
	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.	PRESENT
All-Source Analyst	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
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	PRESENT
	Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.	PRESENT
	Document lessons learned that convey the results of events and/or exercises.	ABSENT
	Advise managers and operators on language and cultural issues that impact organization objectives.	PRESENT

	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.	PRESENT
	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.	PRESENT
	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.	PRESENT
	Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.	ABSENT
	Identify cyber threat tactics and methodologies.	PRESENT
	Identify target communications within the global network.	
	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.	PRESENT
	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.	PRESENT
	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.	PRESENT
	Tip critical or time-sensitive information to appropriate customers.	ABSENT
	Transcribe target voice materials in the target language.	PRESENT
	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).	PRESENT
	Provide near-real time language analysis support (e.g., live operations).	ABSENT
	Identify cyber/technology-related terminology in the target language.	ABSENT

	Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.	PRESENT
	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.	ABSENT
	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
Mission Assessment Specialist	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	ABSENT
	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	PRESENT
	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	PRESENT

	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	PRESENT
	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	PRESENT
	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	PRESENT
	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.	PRESENT
	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	PRESENT
	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	PRESENT
	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures	PRESENT
	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	PRESENT
	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	PRESENT
	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	PRESENT
	Provide leadership in the planning, design and evaluation of privacy and security related projects	ABSENT
	Establish an internal privacy audit program	PRESENT
	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	PRESENT
	Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information	PRESENT
	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	PRESENT
	Review all system-related information security plans to ensure alignment between security and privacy practices	PRESENT
	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	PRESENT
	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	PRESENT

	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	PRESENT
	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	PRESENT
	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	PRESENT
	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	PRESENT
	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 Defense Forensics Analyst	Develop and maintain appropriate communications and training to promote and educate all workforce members and members of the Board regarding privacy compliance issues and requirements, and the consequences of noncompliance	PRESENT
	Determine business partner requirements related to the organization's privacy program.	ABSENT
	Establish and administer a process for receiving, documenting, tracking, investigating and taking corrective action as appropriate on complaints concerning the company's privacy policies and procedures.	PRESENT
	Cooperate with the relevant regulatory agencies and other legal entities, and organization officers, in any compliance reviews or investigations.	PRESENT
	Perform ongoing privacy compliance monitoring activities.	ABSENT
	Monitor advancements in information privacy technologies to ensure organization adoption and compliance.	PRESENT
	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
	Appoint and guide a team of IT security experts.	PRESENT

	Collaborate with key stakeholders to establish a cybersecurity risk management program.	ABSENT
	Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework.	PRESENT
	Establish a risk management strategy for the organization that includes a determination of risk tolerance.	ABSENT
	Identify the missions, business functions, and mission/business processes the system will support.	PRESENT
	Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.	ABSENT
	Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system.	PRESENT
	Identify stakeholder assets that require protection.	ABSENT
	Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis.	PRESENT
	Define the stakeholder protection needs and stakeholder security requirements.	ABSENT
	Determine the placement of a system within the enterprise architecture.	PRESENT
	Identify organization-wide common controls that are available for inheritance by organizational systems.	ABSENT
	Conduct a second-level security categorization for organizational systems with the same impact level.	PRESENT
	Determine the boundary of a system.	ABSENT
	Identify the security requirements allocated to a system and to the organization.	ABSENT
	Identify the types of information to be processed, stored, or transmitted by a system.	PRESENT
	Categorize the system and document the security categorization results as part of system requirements.	ABSENT
	Describe the characteristics of a system.	PRESENT
	Register the system with appropriate organizational program/management offices.	ABSENT
	Select the security controls for a system and document the functional description of the planned control implementations in a security plan.	PRESENT
	Develop a strategy for monitoring security control effectiveness; coordinate the system-level strategy with the organization and mission/business process-level monitoring strategy.	ABSENT
	Review and approve security plans.	PRESENT
	Implement the security controls specified in a security plan or other system documentation.	ABSENT
	Document changes to planned security control implementation and establish the configuration baseline for a system.	PRESENT

	Develop, review, and approve a plan to assess the security controls in a system and the organization.	ABSENT
	Assess the security controls in accordance with the assessment procedures defined in a security assessment plan.	PRESENT
	Prepare a security assessment report documenting the issues, findings, and recommendations from the security control assessment.	ABSENT
	Conduct initial remediation actions on security controls based on the findings and recommendations of a security assessment report; reassess remediated controls.	PRESENT
	Prepare a plan of action and milestones based on the findings and recommendations of a security assessment report excluding any remediation actions taken.	PRESENT
	Assemble an authorization package and submit the package to an authorizing official for adjudication.	PRESENT
	Determine the risk from the operation or use of a system or the provision or use of common controls.	ABSENT
	Identify and implement a preferred course of action in response to the risk determined.	ABSENT
	Determine if the risk from the operation or use of the system or the provision or use of common controls, is acceptable.	PRESENT
	Monitor changes to a system and its environment of operation.	ABSENT
	Assess the security controls employed within and inherited by the system in accordance with an organization-defined monitoring strategy.	ABSENT
	Respond to risk based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in a plan of action and milestones.	PRESENT
	Update a security plan, security assessment report, and plan of action and milestones based on the results of a continuous monitoring process.	PRESENT
	Report the security status of a system (including the effectiveness of security controls) to an authorizing official on an ongoing basis in accordance with the monitoring strategy.	ABSENT
	Review the security status of a system (including the effectiveness of security controls) on an ongoing basis to determine whether the risk remains acceptable.	PRESENT
	Implement a system disposal strategy which executes required actions when a system is removed from service.	ABSENT
	Sponsor and promote continuous monitoring within the organization.	PRESENT
	Assign staff as needed to appropriate continuous monitoring working groups.	ABSENT
	Identify reporting requirements to support continuous monitoring activities.	PRESENT
	Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.	ABSENT

	Determine how to integrate a continuous monitoring program into the organization's broader information security governance structures and policies.	PRESENT
	Use continuous monitoring scoring and grading metrics to make information security investment decisions to address persistent issues.	PRESENT
	Ensure that the continuous monitoring staff have the training and resources (e.g., staff and budget) needed to perform assigned duties.	ABSENT
	Work with organizational risk analysts to ensure that continuous monitoring reporting covers appropriate levels of the organization.	PRESENT
	Work with the organizational risk analysts to ensure risk metrics are defining realistically to support continuous monitoring.	ABSENT
	Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels.	ABSENT
	Establish triggers for unacceptable risk thresholds for continuous monitoring data.	PRESENT
	Work with organizational officials to establish system level reporting categories that can be used by the organization's continuous monitoring program.	ABSENT
	Designate a qualified person to be responsible for the management and implementation of the continuous monitoring program.	PRESENT
	Identify the continuous monitoring stakeholders and establish a process to keep them informed about the program.	ABSENT
	Identify security oriented organization reporting requirements that are fulfilled by the continuous monitoring program.	PRESENT
	Use the continuous monitoring data to make information security investment decisions to address persistent issues.	ABSENT
	Define triggers within the continuous monitoring program that can be used to define unacceptable risk and result in action being taken to resolve.	PRESENT
	Establish scoring and grading metrics to measure effectiveness of continuous monitoring program.	ABSENT
	Work with security managers to establish appropriate continuous monitoring reporting requirements at the system level.	PRESENT
	Use the continuous monitoring tools and technologies to assess risk on an ongoing basis.	ABSENT
	Establish appropriate reporting requirements in adherence to the criteria identified in the continuous monitoring program for use in automated control assessment.	ABSENT
	Use non-automated assessment methods where the data from the continuous monitoring tools and technologies is not yet of adequate sufficiency or quality.	PRESENT

	Develop processes with the external audit group on how to share information regarding the continuous monitoring program and its impact on security control assessment.	ABSENT
	Identify reporting requirements for use in automated control assessment to support continuous monitoring.	PRESENT
	Determine how the continuous monitoring results will be used in ongoing authorization.	ABSENT
	Establish continuous monitoring tools and technologies access control process and procedures.	ABSENT
	Ensure that continuous monitoring tools and technologies access control is managed adequately.	PRESENT
	Establish a process to provide technical help to continuous monitoring mitigators.	ABSENT
	Coordinate continuous monitoring reporting requirements across various users.	PRESENT
	Establish responsibilities for supporting implementation of each continuous monitoring tool or technology.	ABSENT
	Establish liaison with scoring and metrics working group to support continuous monitoring.	PRESENT
	Establish and operate a process to manage introduction of new risk to support continuous monitoring.	ABSENT
	Establish continuous monitoring configuration settings issues and coordination sub-group.	ABSENT
	Establish continuous monitoring tools and technologies performance measurement/management requirements.	PRESENT
	Using scores and grades to motivate and assess performance while addressing concerns to support continuous monitoring	ABSENT
	Work with security managers (i.e., system owners, information system security managers, information system security officers, etc.) to establish appropriate reporting requirements for continuous monitoring at the system level.	PRESENT
	Use continuous monitoring tools to assess risk on an ongoing basis.	ABSENT
	Use the continuous monitoring data to make information security investment decisions to address persistent issues.	PRESENT
	Respond to issues flagged during continuous monitoring, escalate and coordinate a response.	ABSENT
	Review findings from the continuous monitoring program and mitigate risks on a timely basis.	PRESENT

List of potential threats to Symetrica that could exploit vulnerabilities of critical assets due to missing Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks:

- Retrieval of unauthorized data and Man-In-The-Middle attack
- Full control of architecture, unable to access any machine.
- Buffer overflows attacks
- Illegitimate data transfer attacks, Denial of Service attacks.
- Elevated privileges attacks, Credential theft attacks, Data interception
- Server and other critical assets attacks, Malware or other malicious code uploads.
- Sniffing and wireless scanning attacks, piggybacking & network reconnaissance Attacks
- Network Layer attacks, social engineering attacks, retrieval of unauthenticated data, website cookie exploitation and overriding authenticated sessions- session hijacking
- DOS attacks, Arbitrary code execution slow system memory leak
- Remote code execution, Flood attacks to harm system's availability.
- Loss of Data Privacy and Confidentiality, Retrieval of unauthorized data and Man-In-The-Middle attack
- Credential theft attacks, information theft
- Unauthorized access, Credential theft attacks
- Evil Twin attacks, Retrieval of unauthorized data and Man-In-The-Middle attack
- Outbound email attacks and Eavesdropping attacks.

List of potential risks for critical assets where Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks are missing

- Data Breaches, unauthorized access might result in damage and installation of malware on systems.
- Exhaustion of resources of affected systems, memory exhaustion resulting in unexpected reloads.
- Full system compromise, Manipulation of sensitive information in lo files.
- Weak network infrastructure, attackers maintain persistence within the network
- loss of control of infrastructure backbone,
- unauthorized access might result in damage and installation of malware on systems.
- Escalated root access, user accounts data exposure.
- Installation of malware on endpoints, manipulation of data.
- unauthorized access might result in damage and failed access controls
- Remote code execution, inability to identify the breach
- Unauthorized folders and data access, read, update or delete data
- Infect systems laterally connected and block legitimate Bluetooth traffic.
- Masquerading as an authorized user & data modification

- unauthorized access might result in damage and installation of malware on systems.
- Cause interruption of operations due to authenticating non trusted access
- Result in operating system attacks and unavailability of services
- Result in network related attacks, improper functioning of infrastructure & non-compliance
- Unauthorized Access might result in damage and loss of physical assets
- Deteriorating the throughput of network's links, possibility of DOS attacks and unavailability of services

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

- Security Awareness Training programs highlighting the higher probability threats can be made more frequent.
- Configuration management, user awareness training and Bluetooth awareness policy shall help mitigate Bluetooth related risks to greater extent.
- By applying such various countermeasures, it is also necessary to test the incident response plan periodically to evaluate the effectiveness and update the plan accordingly.
- Document, review and update the Disaster recovery, Business continuity and continency plans.
- Harden the network management devices by using strong password policies and disabling unnecessary management services on the devices.

Part C Security Risk Management Recommendations

Security Risk Management Recommendations for HGA

- Along with the current controls in place for HGA and the new controls recommended by CISO, additional controls of implementing VPN and DMZ have strengthened the security posture of HGA.
- Although HGA has effectively implemented few of the response controls by using redundant servers and stronger password policy, relevant to the controls listed in Common Criteria, it needs to look more into strengthening of Audit Accountability, Configuration Management and Supply Chain Risk Management Controls.
- Additional risk management controls can be implemented such as restricting attempts for passwords and restriction of services that impact operational effectiveness.
- Additional risk management controls can be implemented such as restricting non-essential services and implementing periodic review of the access controls.
- Implementation of redundant servers can help to mitigate this vulnerability to greater extent.
- HGA has effectively implemented few of the controls relevant to the controls listed in Common Criteria, it doesn't look into Environment Protection, Personnel Security and Supply Chain Risk Management Controls.
- Additional hardening controls can be implemented such as implementing VLANS to mitigate "in the clear" conversations.
- Implementation of Multi Factor Authentication with biometrics/ security device can also help to mitigate this vulnerability and also the other vulnerabilities to greater extent.
- Additional controls can be implemented such as implementing advanced encryption methods for communication to servers and on PC hard disks.
- Implementation of IPS along with routinely updating the signatures can help to mitigate this vulnerability to greater extent.

Security Risk Management Recommendations for Symetrica:

- Controls strengthening Incident Response Capabilities need to be implemented.
- Periodically reviewing the effectiveness of Security Controls can help strengthen the controls in place and reduce the probabilities of vulnerabilities.
- Intrusion Prevention Systems and regular update of digital signatures need to be done to proactively mitigate uprising threats.
- Patches need to be regularly checked, tested in an isolated environment and patched.
- Audit Trails control can be implemented and reviewed to identify potential service and process problems.
- Intermittently test the security configurations, backup the configurations and store them offline.
- Continually monitor and assess the security of management and critical systems, networks and infrastructure.
- Test backups of the system consistently and schedule operating system patches and hardware firmware patches at routine intervals.

- SIEM technology can be integrated to integrate multiple log formats from different sources and generate alerts on identified traffic patterns.
- By applying such various countermeasures, it is also necessary to test the incident response plan periodically to evaluate the effectiveness and update the plan accordingly.
- Monitor and log networking devices and verify their configurations schedule periodically.
- Manage and store the access information of networking devices by using Authentication, Authorization and Accounting services, to limit the access and only required privileges to the user.
- Document, review and update the Disaster recovery, Business continuity and continency plans.
- Reviewing and monitoring the log files of networking devices, can help in identifying potential exploitation attempts, to harden the networking devices
- Implement backup solutions to automatically back up critical data and keep the backup data in a secure and remotely isolated environment.
- Implement security checklist to audit and harden the application configurations and allow only the application modules and services that are required as per business needs.
- Audit the code and services that are being provided by third-party while not being hosted on the server to ensure that there is no invalidated code being delivered.
- Blocking the most commonly exploited wireless attacks identified in this plan along with detection and reporting of any additional attacks can strengthen the prevention control capabilities.
- Generate automated event triggering, event log capturing and creation of customizable reports.

Provide the total cost and benefit in $ for the recommended controls, methods and policies based on your security risk management analysis

For HGA:
The Budget for proposed controls:

Residual Risk= Risk with current controls- Risk with new controls
1,174,000 – 4,972 = 1,169,028

Proposed Security Budget Cost for 3 budgets:

- ➔ Cost benefit ratio analysis for risk prevention budget
    - o Proposed Security Risk Budget cost/ expected security risk benefit
      = 220,000 / 1,169,028 = 0.19

- ➔ Cost benefit ratio analysis for risk response budget
    - o Proposed Security Risk Budget cost/ expected security risk benefit
      = 305,000 / 1,169,028 = 0.26

- ➔ Cost benefit ratio analysis for risk response budget
    - o Proposed Security Risk Budget cost/ expected security risk benefit

= 470,000 / 1,169,028 =0.4

For Symetrica:

Residual Risk with current controls= $500,000
Residual Risk with new controls= $75,000

Proposed Security Budget Cost: $300,000

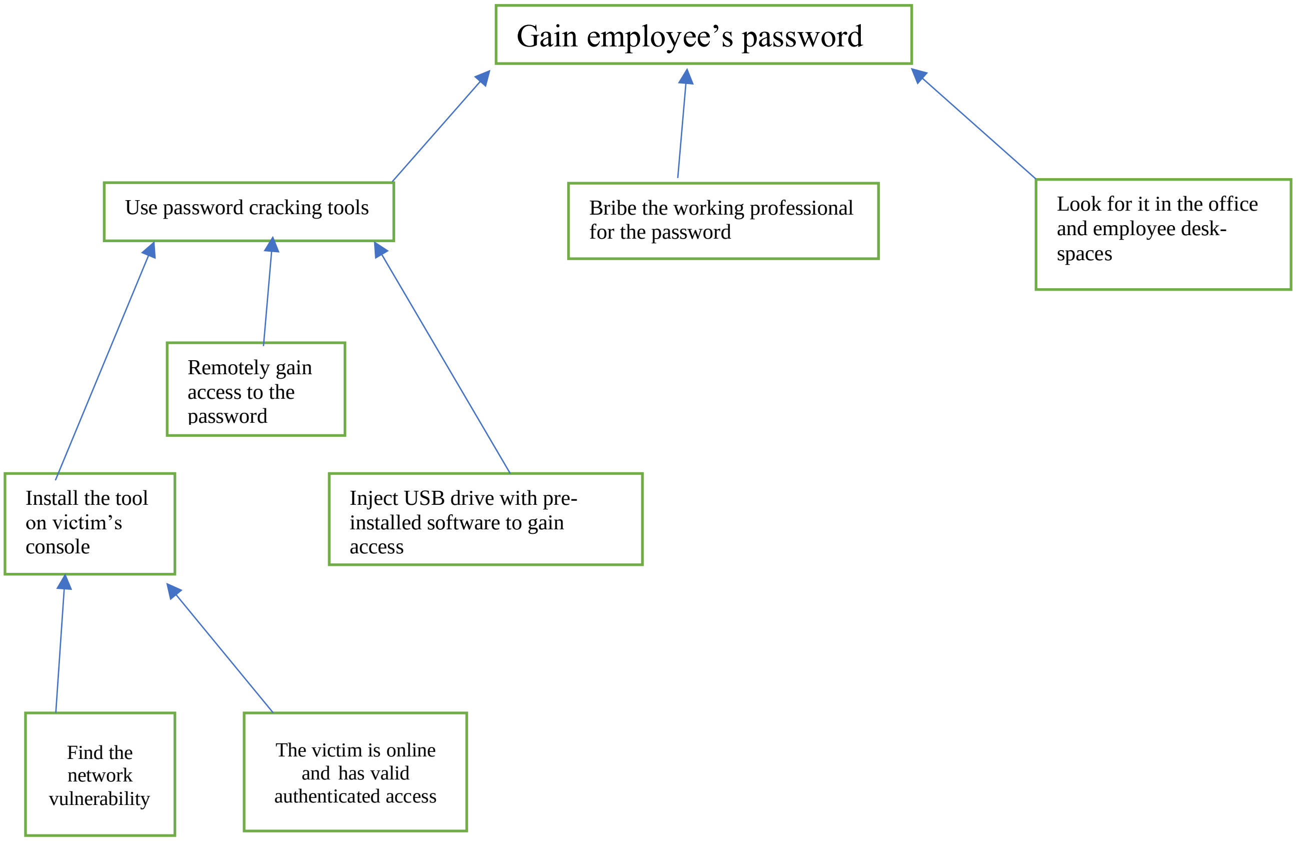
Residual Risk= Risk with current controls- Risk with new controls
= 500,000-75,000= 425,000
Proposed Security Budget Cost for 3 budgets:

- ➔ Cost benefit ratio analysis for proposed budget
    - o Proposed Security Risk Budget cost/ expected security risk benefit
      = 300,000/425,000
      =0.71

Comparison of proposed security controls, methods and policies budget for HGA with the proposed security controls, methods and policies budget for Symetrica:

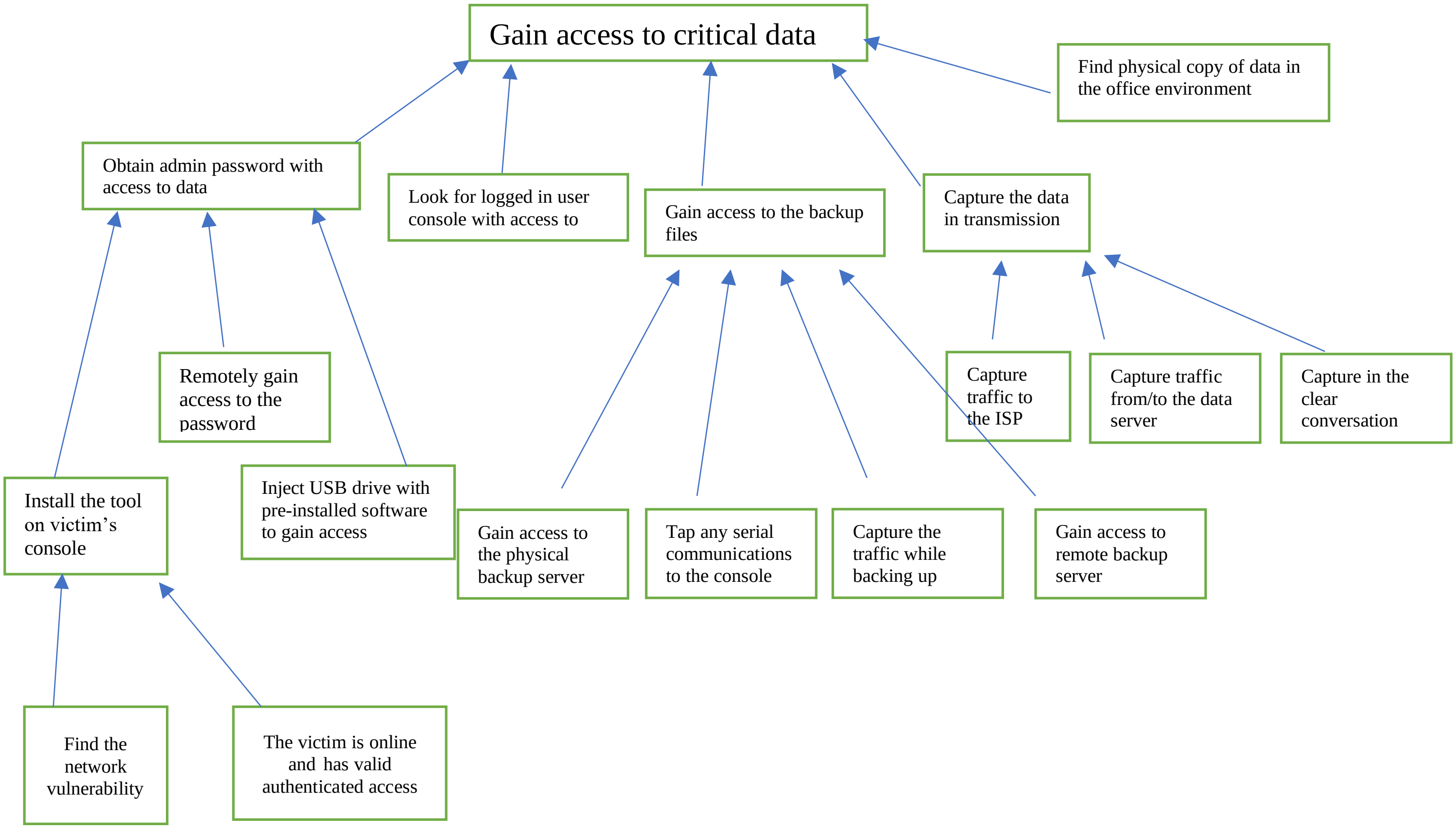
Security Risk Management Areas	HGA	Symetrica
Industry	Financial company	design and manufacturing company
Mission	Transfer U.s government funds in form of paychecks to individuals	To provide the very best overarching threat detection and identification solutions to facilitate the security teams to make smart decisions in multi-threat situations.
Geographic Presence	United States of America	United States of America, United Kingdom
Number of Employees	500	100
Network Topology	Appendix 3	Appendix 4
Critical Assets in $	274,000	$725,000
Attack Tree Scenarios		
Threat Agent	State sponsored, hacker group threat agents	Terrorist and Criminal group threat agents
Residual Security Risk in $	$1,169,028	$425,000
Budget for Risk Prevention and response controls, methods, policies	$470,000	$300,000
$ security budget / $ security risk improvement	0.4	0.7
$ security budget / $ critical assets	0.17	0.41
$ security budget / employee	548	3000

HGA ATTACK TREE SCENARIO


Gain employee's password
Use password cracking tools
Bribe the working professional for the password
Look for it in the office and employee desk-spaces
Remotely gain access to the password
Install the tool on victim's console
Inject USB drive with pre-installed software to gain access
Find the network vulnerability
The victim is online and has valid authenticated access

\

SYMETRICA ATTACK TREE SCENARIO


Gain access to critical data
Find physical copy of data in the office environment
Obtain admin password with access to data
Look for logged in user console with access to
Gain access to the backup files
Capture the data in transmission
Remotely gain access to the password
Capture traffic to the ISP
Capture traffic from/to the data server
Capture in the clear conversation
Install the tool on victim's console
Inject USB drive with pre-installed software to gain access
Gain access to the physical backup server
Tap any serial communications to the console
Capture the traffic while backing up
Gain access to remote backup server
Find the network vulnerability
The victim is online and has valid authenticated access

Threats exploiting vulnerabilities-poetntail
Workforce recomm
Topology diags- explanantion.

VULNERABILITIES AND EXPLOITATION PROBABILITIES FOR HGA:

Vulnerability Name	PROBABILITY
Unauthorized Access	25
Virus Prevention	15
Vulnerabilities Related to disclosure or brokerage of information	20
Vulnerabilities related to Network Related Attacks	10
Heap buffer overflow vulnerability	25
Payroll Fraud	25
Interruption of operations	15
Disclosure or Brokerage of Info	10
Network- Related attacks	15
Man-In-The-Middle attack	20

VULNERABILITIES AND EXPLOITATION PROBABILITIES FOR SYMETRICA:

Vulnerability Name	PROBABILITY
Vulnerabilities Related to authentication logic and Insecure session handling	45
vulnerabilities related to internal corporate attacks and disclosure or brokerage of information	25
Unauthorized Access and missing lock out process	50
Vulnerabilities related to Unauthorized Access, Vulnerabilities Related to Interruption of Operations	25
Vulnerabilities Related to access control, vulnerabilities related to IP addresses, ports and services disclosure.	45
vulnerabilities related to malicious traffic, website breaches and data exfiltration	45
Rogue WIFI Access Points (WAPS), Vulnerabilities related to non-encrypted 802.11 traffic	50
Private IP Address disclosure, malicious software related attacks	45
Improper memory resource management, missing input validation, improper error handling	25
Improper filtration of serialized input, improper implementation of mechanisms to prevent DOS attacks.	45
Unauthorized access, network reconnaissance	45
Unauthorized infrastructure access, administrative privileges exploitation	25
Unauthenticated arbitrary file disclosure	45
Cipher transmission insecure, sensitive data exposure.	25
Installation of malware, improper certificate validation,	50

Broken authentication, Session ID leakage, Unrestricted file uploads	25
Directory indexing, insufficient session expiration	25
Excess privilege assigned to accounts, security misconfigurations,	45
Unvalidated automatic library activation, Insufficient auditing and logging.	25

WORKFORCE RECOMMENDATIONS FOR HGA:

- Security Awareness and training highlighting the most exploited vulnerabilities is recommended
- Personnel background check and Identification access management needs to be reviewed periodically
- All the policies that identified and assigns various roles and responsibilities, are required to be reviewed and approved by the identified personnel.
- Implementation of process of approval and review of policies being developed is recommended

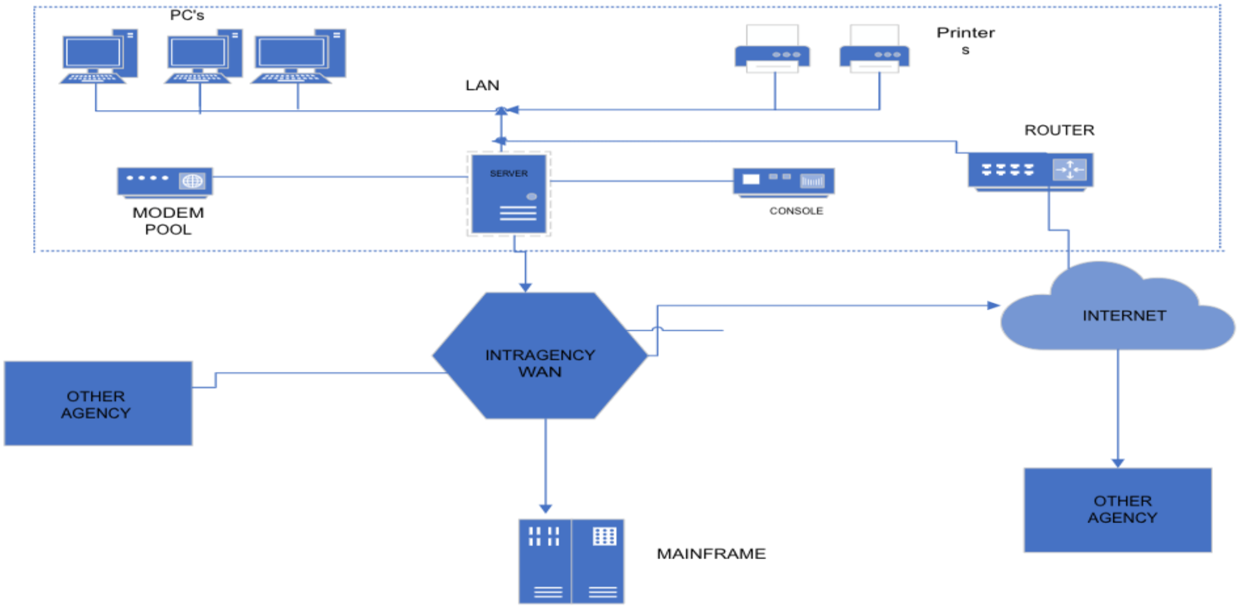
WORKFORCE RECOMMENDATIONS FOR SYMETRICA:

- Manage and store the access information personnel by using Authentication, Authorization and Accounting services, to limit the access and only required privileges to the user.
- Document, review and update the Disaster recovery, Business continuity and continency plans.
- Implementing security awareness and training highlighting the most exploited vulnerabilities is recommended
- Participation of personnel in incident response plan testing exercise, helps them gain more knowledge on business continuity plans for the company.
- Implement security checklist to audit and harden the security controls to ensure the cybersecurity posture implemented is up to date.
- Audit the code and services that are being provided by third-party while not being hosted on the server to ensure that there is no invalidated code being delivered.
- Generate automated event triggering, event log capturing and creation of customizable reports.

PART-D APPENDIX

APPENDIX- 3

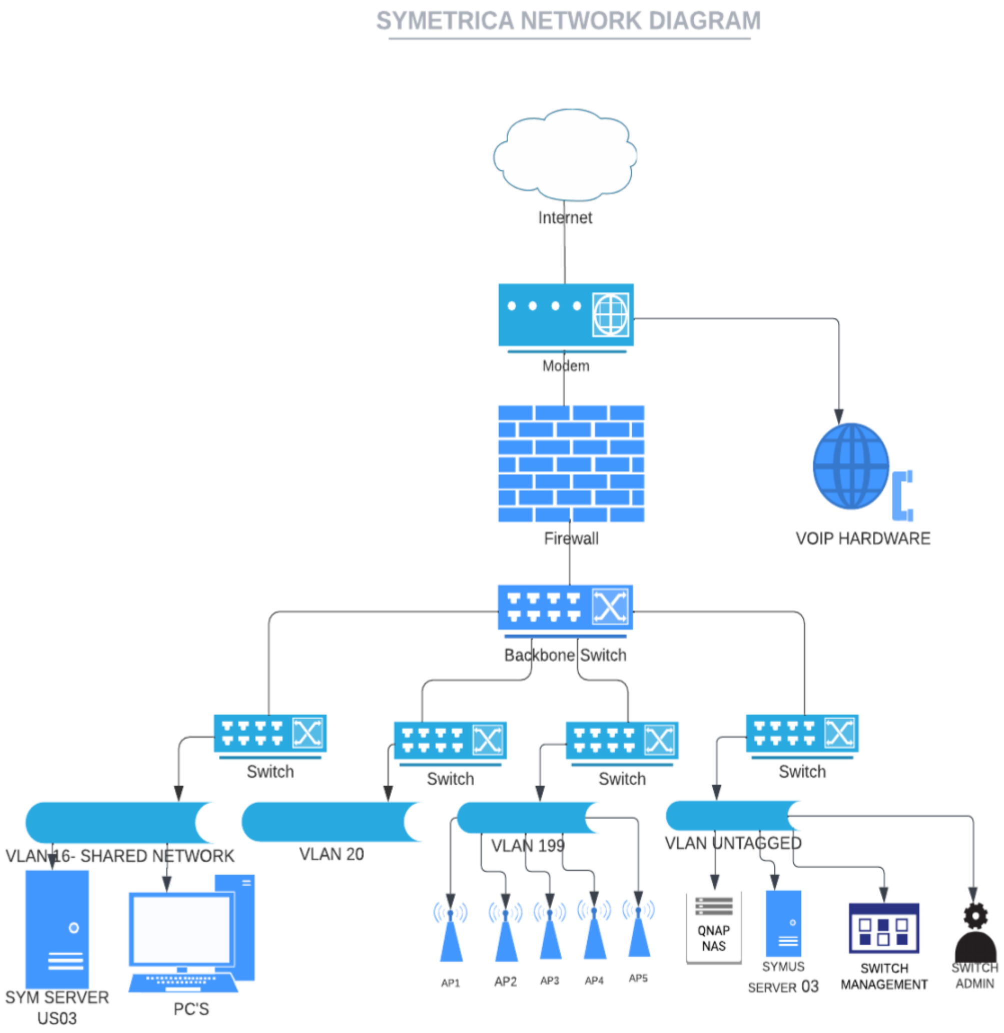
NETWORK TOPOLOGY FOR HGA



The network topology describes the distributed system architecture of HGA. This diagram helps in identifying and scoping the assets owned by HGA which are going to be evaluated in the security risk analysis. It also helps in identifying the neighboring assets, their ownership and potential risks posed by such. As seen in the network diagram the LAN server acts as the central component of the architecture. As the router, printers, computers, modem pool and special console are directly being connected to the LAN server.

APPENDIX- 4

NETWORK TOPOLOGY FOR SYMETRICA



The network topology describes the enterprise architecture for Symetrica. As a small enterprise with limited number of employees, Symetrica has implemented basic network architecture where the firewall acts as the primary control. All the critical assets, the servers and the workstations of the company are located on their own secure VLANs to secure the communications within the company.

REFERENCES:

→ The Security Risk Assessment Handbook, 2nd Edition, Landoll, Chapter 1, Introduction https://www.oreilly.com/library/view/the-security-risk/9781439821497/

→ Chapter 20 from National Institute of Standards and Technology (NIST) SP 800-12, “Assessing and Mitigating the Risks to a Hypothetical Computer System”

→ RISK MANAGEMENT FOR COMPUTER SECURITY, Andy Jones and Debi Ashenden, 2005, Chapter 5 and 6

→ Module-06 Presentation

→ Security Concerns in Naval Accesshttps://apps.dtic.mil/sti/pdfs/ADA620829.pdf

→ Securing Network Infrastructure Devices https://www.cisa.gov/uscert/ncas/tips/ST18-001

→ CISA guidelines for application vulnerabilities and their preventive controls from, https://www.cisa.gov/uscert/ncas/tips/ST18-006