CY5200

SECURITY RISK MANAGEMENT AND ASSESSMENT

FINAL REPORT

STUDENT: KOLAVASI VAISHNAVI

TABLE OF CONTENTS

PART A) SECURITY RISK MANAGEMENT AND ASSESSMENT

EXECUTIVE SUMMARY

Name of the information system: Hypothetical Government Agency (HGA)

Categorization of the information system:

ASSETS	INFORMATION SECURITY ELEMENTS		
	CONFIDENTIALITY (C)	**INTEGRITY (I)**	**AVAILABILITY (A)**
Contract documents	M	H	M
Draft regulation	M	H	M
Memos	H	H	H
Personal computers	H	H	H
Hard disk	H	H	H
LAN Server	H	H	H
Router	H	H	H
Modem pool	H	H	H
Special console	H	H	H

High	–: H
Medium	–: M
Low	–: L

Name of the organization: Hypothetical Government Agency (HGA)

Address of the organization: 100 Saint Alphonsus street, Boston, Massachusetts – 02120

Abhishek A Kumar

Designation: Chief executive officer

Email-id: abhishekAK@gmail.com

Phone: +1 924 565 4344

Harshitha

Designation: Chief Information officer

Email-id: harshitha12@gmail.com

Phone: +1 923 564 4364

Ujwala

Designation: Chief Financial officer

Email-id: ujwala127@gmail.com

Phone: +1 605 554 4867

Bindu

Designation: Chief Information Security Officer

Email-id: Bindu090@gmail.com

Phone: +1 878 564 6360

Operational status of the information system: Active (Operational)

Type of the information system: Major application

System description: It transfers the funds received from the US government to the individuals.

Interconnection of system information:

System Name: Government agency

Organisation type: Public sector Telecommunications industry

Agreement type: Government contract

Date: 22nd July 1997

FIPS 199 Category: High

C&A category: Accredited and Certified

Authorizing official: Harshitha

The list of applicable laws/framework/ standards/ policies/ regulations:

1. Appendix III to OMB Circular A-130, the Computer Security Act of 1987, and the Privacy Act
2. Policies based on OMB Circulars A-123 and A-127.

3. Federal Managers' Financial Integrity Act
4. Privacy act
5. Sarbanes Oxley Act of 2002
6. Federal Risk and Authorization Management Program (FedRAMP)

PART III) let’s assume the total number of employees working in HGA is 100. The HGA financial resources account for 400000, the value of the confidential information such as employee data of HGA is 200000 and, the value of the draft regulations, contract documents, and memos is 100000 each respectively.

The number of assets and total value including their maintenance cost is listed below:

Financial resources (A_1) - $400000

Employee information (A_2) - $200000

ASSET NAME AND NUMBER	NUMBER OF ASSETS	VALUE OF EACH	TOTAL VALUE
Contract documents (A_3)	100	$1000	100*1000=$100000
Draft regulations (A_4)	100	$1000	100*1000=$100000
Memos (A_5)	1000	$100	1000*100=$100000
Personal computers (A_6)	300	$700	300*700=$210000
Hard disk (A_7)	150	$50	150*50=$7500
LAN Server (A_8)	10	$3000	10*3000=$30000
Router (A_9)	20	$100	20*100=$2000
Street	20	$400	20*400= $8000
Special Console (A_{11})	30	$20	30*20=$ 600

- Threats associated with the assets:
    1. Payroll fraud (T_1): discrepancies observed in sick leaves availed, timesheets submitted, advances taken and various other fields in the payroll generated contribute to payroll fraud.
    2. Payroll errors (T_2): Incorrect entry of details in the payroll time and attendance section, failure to eliminate and update the former and new employees’ details respectively, loss of employee time data constitute payroll errors.
    3. Interruptions in the operations (T_3): The antediluvian facilities and physical plant of the agency are prone to a disturbance in their functioning. As a result, the various facilities reliant on them like AC, power, LAN, and WAN experience irregular and improper functioning as well.
    4. Natural calamities (T_4): Fire accidents, floods, and storms can obstruct regular computer functioning.
    5. Equipment malfunctioning (T_5): Improper handling and maintenance of equipment can cause wear and tear.
    6. Intruder or outsider threat (T_6): This occurs when an intruder or employee having no access to services or a particular portion of company data, gains

access to such data or documents (confidential) of the agency and is capable of performing any modifications to them, introducing new software applications containing malware into the personal desktops of the employees, stealing confidential information from the company database and, modifying the configuration settings of the access controls.

7. Revealing information (T_7): Observed when the employees reveal the company information describing its internal functions to the opponents in greed of money or any other aspects.
8. Network associated threats (T_8): The 3 external networks to which the HGA systems are connected are prone to threats such as unauthorized access or modifications to the company data and privileges.
9. Theft (T_9): This includes loss of documents due to robbery.

- Vulnerabilities Possible:

1. Corrupted timesheets (V_1): Altering working hours in timesheets leads to manipulation in the timesheet data.
2. Unauthorized access (V_2): A malicious code would brute-force passwords that are being sent to the server for the authorization process thereby leading to unauthorized access to the application intended.
3. Unapproved modification of payroll data (V_3): This denotes modification of files containing payroll data. And also, switches present in WAN that are responsible for data exchange between network devices are susceptible to illegal modification of payroll data.
4. Mainframe I&A system (V_4): As the Identity and Access Management system used is password-based, it possesses a possibility for vulnerability as various attacks such as brute force, credentials' stuffing can be used to intercept and find the password thus granting illegal authorization to data and resources.
5. Incomplete contingency planning (V_5)
6. Unemployed virus prevention strategies (V_6)
7. Loss of data due to lack of backup (V_7)
8. Unsecure storage of confidential information
9. Communication of unencrypted data over a network (V_9)

Minimum security controls:

MOT control number	Security Control	Observation	Status	Content-type	Authority responsible
1	Data security-related issues.	Computer system policies employed and followed are inclined towards payroll.	Partial	Common	CISO
2	Managing the accessibility of data based on its type and confidentiality.	Data access is given to the officials who only need to have access based on the requirement of the work.	Partial	Common	CIO
3	Restrictions on sharing of credentials.	Employees are refrained from sharing their credentials even with their colleagues.	Complete	Common	CISO
4	Mandatory security awareness training or live interactive course for new employees.	To acquaint with the security of the company, it is mandatory for any new joiner to complete security awareness training or a live interactive session.	Complete	Common	CISO
5	Backup of time and attendance data.	The time and attendance data is taken as a backup every night to avoid loss of data.	Partial	Common	CIO
6	Contingency planning	Develop and test contingency plans annually	Complete	Common	CIO

		to discover individuals and resources needed to ensure the continuity of organizations' operations.			
7	Preventing unauthorized access of data.	Automated access control to decrease unauthorized access and corruption of time and attendance data accidentally.	Complete	Common	CISO
8	Data integrity verification	Application on the LAN server that checks the correctness and validity of the time and attendance data.	Complete	Common	CIO
9	Protection against viruses.	Authorized system administrators are allowed to install COG approved licensed, copyrighted packages for PC to protect them from viruses.	Complete	Common	CISO
10	Translating network traffic	Traffic is filtered and managed on the network by the use of firewall.	Partial	Common	CIO
11	Data encryption	Encryption of data sent and received to the LAN hardware to protect against intruders.	Partial	Common	CISO

Information security plan complete date: 04/ 04/2022
Information security plan approval date: 22/07/2022

- A subset of assets:

  A_1: Financial resources- $400000

  A_2: Employee information- $200000

  A_6: Personal computers-$210000

  A_7: Hard disk-$7500

  $A_{12:}$ VPN server - $3000

  A_{13}: DMZ - $20000

- A subset of threats:

  T_1: Payroll fraud

  T_2: Payroll error

  T_5: Equipment malfunctioning

  T_7: Revealing information

  T_9: Theft

- A subset of vulnerabilities:

  V_1: Corrupted timesheets

  V_2: Unauthorized access

  V_8: Unsecure storage of confidential information

  V_9: Communication of unencrypted data over a network

- Asset-vulnerability pairs:

  Financial resources (A_1):

  i. V_1: Corrupted timesheets
  ii. V_2: Unauthorized access
  iii. V_8: Unsecure storage of confidential information
  iv. V_9: Communication of unencrypted data over a network

  Employee information (A_2):

i. V_2: Unauthorized access
ii. V_8: Unsecure storage of confidential information

Personal computers (A_6):

i. V_2: Unauthorized access
ii. V_9: Communication of unencrypted data over a network

Hard disk (A_7):

i. V_8: Unsecure storage of confidential information

Management	Operational	Technical
Computer system policies employed and followed are inclined towards payroll data security-related issues. ($MOT_{1)}$	Restrictions on sharing of credentials. ($MOT_{3)}$	Automated access control to decrease unauthorized access and corruption of time and attendance data accidentally. ($MOT_{7)}$
Managing the accessibility of data based on its type and confidentiality. ($MOT_{2)}$	Mandatory security awareness training or live interactive course for new employees. ($MOT_{4)}$	Application on the LAN server that checks the correctness and validity of the time and attendance data. ($MOT_{8)}$
	Backup of time and attendance data. ($MOT_{5)}$	Authorized system administrators are allowed to install COG approved licensed, copyrighted packages for PC to protect them from viruses. ($MOT_{9)}$
	Develop and test contingency plans annually to discover individuals and resources needed to ensure the continuity of organizations' operations. ($MOT_{6)}$	Traffic is filtered and managed on the network by the use of a firewall. (MOT_{10}).
	Encryption of data sent and received to the LAN hardware to protect against intruders. ($MOT_{11).}$	

- Current security controls and policies:

1. Use and administration of computer system:

a. Only system administrators have the authority to issue login credentials to the network devices across the LAN server.

MOT control: 7

b. All new users are expected to complete a security and awareness training course or an interactive training session to understand their security responsibilities and need to acknowledge the same in writing.
MOT control: 4

c. The authorized users are issued private login credentials which are refrained from sharing
MOT control: 2, 3, 7

d. The accessibility of confidential information is to be restricted to authorized personnel
MOT control: 3, 9, 11

2. Payroll Fraud:
   a. Categorizing and restricting the readability of the employee's personal information.
   MOT control: 1, 2, 3, 11

   b. Maintaining accurate and up-to-date data of the employee.
   MOT control: 5, 8, 9

   c. Verifying the accuracy of the employees and their time and attendance information by at least 2 other authorized employees.
   MOT control: 8

   d. Only the authorized supervisors can approve, modify or submit the time and attendance data of other individuals.
   MOT control: 2, 5

   e. Safeguarding against unapproved access or updating of time and attendance data by making the application execute on the server wherein using the PC as an intermediary between server and user.
   MOT control: 2, 7, 9, 10, 11

3. Payroll Errors:
   a. The practice of re-entering time and attendance data and comparison of the 2 output files has been followed to reduce the probability of having payroll errors.

4. Accidental corruption or loss of data:
   a. This is prevented by access-control highlights of the server and mainframe working framework

MOT control: 5, 7, 8

b. A backup of data is performed every night which can be handy at times of unavoidable circumstances leading to adulteration or loss of data.
MOT control: 5, 8

c. Ensuring that the time and attendance data are timely presented by various divisions.
MOT control: 6

5. Operation interruptions:
The units of HGA must devise unit-specific contingency plans which explain their reliability of them on various resources and applications, thereby also stating the amount of time that resource can malfunction without having an impact on the operations and services of the divisions.
MOT control: 6

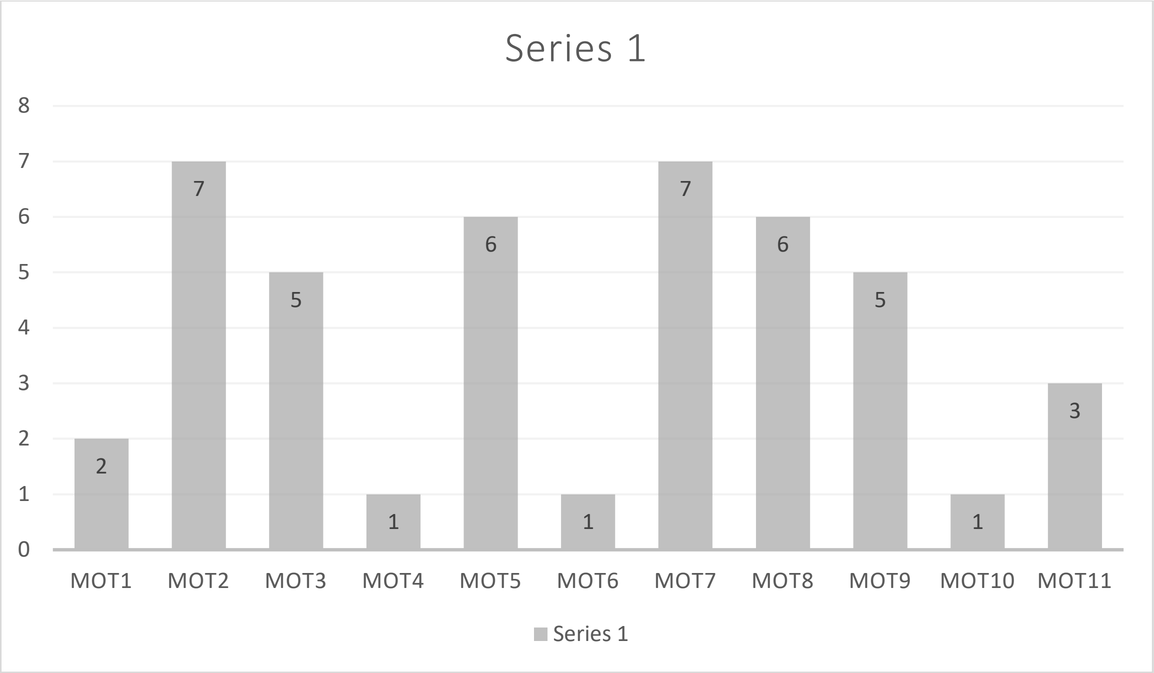
6. Disclosure of information:
A stringent recruitment process can alleviate the risk of revealing the internal information of the agency.
MOT control: 1, 2, 3

7. The need-to-know policy proposed explains various rules to abide by such as securely storing the time and attendance data in secured cabinets and hard disks, providing access to confidential information to intended employees, etc.
MOT control: 5, 9

8. Network related threats:
The router and LAN segregate and eliminate unauthorized transactions.
MOT control: 2, 7, 8

9. Confining the access of WAN to special access control privileges.
MOT control: 8

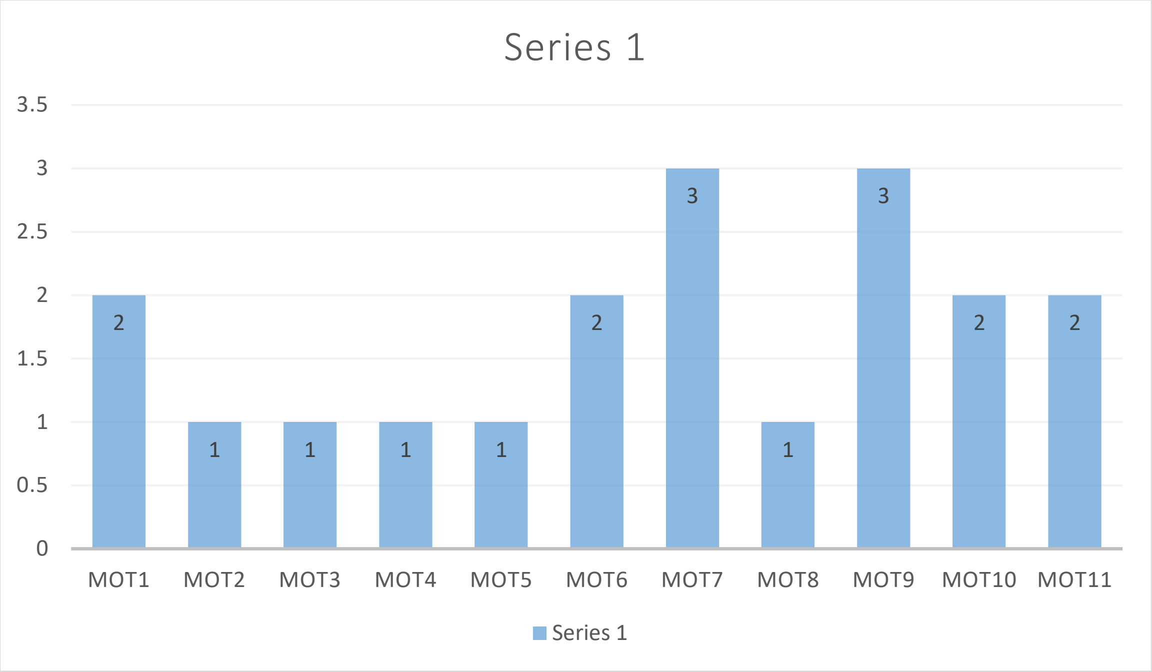
10. Non-HGA computer systems:
These systems should be used to save, process, or transfer data related to the agency only on receiving approval from the application owner and COG (Computer operation group) Manager.
MOT control: 9



- <u>New security controls and policies:</u>
    1. To mitigate payroll fraud:
        a. The use of one-time passwords was proposed to create a secure and robust authentication technique specifically for the users handling highly sensitive information.
        b. Refining and fastening the process of installation of bug fixes linked to security
        c. Use of digital signatures to identify unauthorized access to data.
        MOT control: 1, 2, 3, 7, 9

    2. To safeguard against payroll errors:
        a. Compliance audit regularly.
        b. Using digital signature to verify the authorization of the user.
        MOT control: 1, 7, 9, 11

    3. To ensure continuity of operations:
        a. Examining the sectors whose security policies need to be propagated across the existing and new employees.
        b. Enhanced adherence to the virus prevention techniques.
        c. Regularly analyzing the audit logs of the mainframe system.
        MOT control: 4, 5, 6, 8, 9, 10
    4. Network related threats:
        a. Strengthening the system of Identity and Access management.
        b. The distribution of encrypted modems to every employee.
        MOT control: 6, 7, 10



Security Risk Prevention Strategy P1:

- Initial risk effects: When the worst-case scenario is taken into consideration which implies that the system resilience to threat-vulnerability pair is 0 and the assets have been exploited completely, the scenario looks as mentioned below.

- Threat-vulnerability pairs with probability and also on the subset of assets:

	T_1	T_2	T_5	T_7	T_9
V_1	9	8	6	7	10
V_2	7	6	10	6	5
V_5	10	7	9	7	8
V_8	9	8	10	9	6
V_9	8	6	9	10	5

Total: 195

Residual Asset Security risk:

ASSETS	ASSET VALUE	TOTAL THREAT	RESIDUAL SECURITY RISK
A_1	400000	195	400000*195=78000000
A_2	200000	195	200000*195=39000000
A_6	210000	195	210000*195=40950000
A_7	7500	195	7500*195=1462500
A_{12}	3000	195	3000*195=585000

A_{13}	20000	195	20000*195=3900000

Residual Vulnerability Security Risk:

For V_1: 9+8+6+7+10=40

For V_2: 7+6+10+6+5=34

For V_5: 10+7+9+7+8=41

For V_8: 9+8+10+9+6=42

For V_9: 8+6+9+10+5=38

Substitute the above values accordingly

Risk due to V_1= [(400000*40) + (200000*40) + (210000*40) + (7500*40) + (3000*40) + (20000*40)]/100 =336200

Risk due to V_2= [(400000*34) + (200000*34) + (210000*34) + (7500*34) + (3000*34) + (20000*34)]/100 =285770

Risk due to V_5= [(400000*41) + (200000*41) + (210000*41) + (7500*41) + (3000*41) + (20000*41)]/100=344605

Risk due to V_8= [(400000*42) + (200000*42) + (210000*42) + (7500*42) + (3000*42) + (20000*42)]/100=353010

Risk due to V_9= [(400000*38) + (200000*38) + (210000*38) + (7500*38) + (3000*38) + (20000*38)]/100=319390

Ranking of residual asset risk:

ASSET – RESIDUAL RISK - RANK

A_1	-	78000000	-	1
A_6	-	40950000	-	2
A_2	-	39000000	-	3
A_{13}	-	3900000	-	4
A_7	-	1462500	-	5
A_{12}	-	585000	-	6

Ranking of residual vulnerability security risk:

VULNERABILITY	RESIDUAL RISK	RANK
V_8	353010	1
V_5	344605	2
V_1	336200	3
V_9	319390	4
V_2	285770	5

Security Risk prevention strategy P2:

- Threat-vulnerability pairs with probability and also on the subset of assets:

	T_1	T_2	T_5	T_7	T_9
V_1	8	7	5	6	9
V_2	6	5	9	5	4
V_5	8	6	5	5	7
V_8	6	7	8	8	5
V_9	5	5	6	8	4

Total: 157

Residual Asset Security risk:

ASSETS	ASSET VALUE	TOTAL THREAT	RESIDUAL SECURITY RISK
A_1	400000	157	400000*157=62800000
A_2	200000	157	200000*157=31400000
A_6	210000	157	210000*157=3297000
A_7	7500	157	7500*157=1177500
A_{12}	3000	157	3000*157=471000
A_{13}	20000	157	20000*157=3140000

Residual Vulnerability Security Risk:

For V_1: 8+7+5+6+9=35

For V_2: 6+5+9+5+4=29

For V_5: 8+6+5+5+7=31

For V_8: 6+7+8+8+5=34

For V_9: 5+5+6+8+4=28

Substitute the above values accordingly

Risk due to V_1= [(400000*35) + (200000*35) + (210000*35) + (7500*35) + (3000*35) + (20000*35)]/100 =294175

Risk due to V_2= [(400000*29) + (200000*29) + (210000*29) + (7500*29) + (3000*29) + (20000*29)]/100 =243745

Risk due to V_5= [(400000*31) + (200000*31) + (210000*31) + (7500*31) + (3000*31) + (20000*31)]/100=260555

Risk due to V_8= [(400000*34) + (200000*34) + (210000*34) + (7500*34) + (3000*34) + (20000*34)]/100=285770

Risk due to V_9= [(400000*28) + (200000*28) + (210000*28) + (7500*28) + (3000*28) + (20000*28)]/100=235340

Ranking of residual asset risk:

ASSET –	RESIDUAL RISK	- RANK
A_1 -	62800000	- 1
A_6 -	3297000	- 2
A_2 -	31400000	- 3
A_{13} -	3140000	- 4
A_7 -	1177500	- 5
A_{12} -	471000	- 6

Ranking of residual vulnerability security risk:

VULNERABILITY –	RESIDUAL RISK	- RANK
V_1 -	294175	- 1

V_8	-	285770	-	2
V_5	-	260555	-	3
V_2	-	243745	-	4
V_9	-	235340	-	5

Security Risk prevention strategy P3:

- Threat-vulnerability pairs with probability and also on the subset of assets:

	T_1	T_2	T_5	T_7	T_9
V_1	6	5	4	5	7
V_2	5	5	7	4	3
V_5	6	5	3	4	4
V_8	4	5	6	3	3
V_9	4	4	4	6	4

Total: 116

Residual Asset Security risk:

ASSETS	ASSET VALUE	TOTAL THREAT	RESIDUAL SECURITY RISK
A_1	400000	116	400000*116=46400000
A_2	200000	116	200000*116=23200000
A_6	210000	116	210000*116=24360000
A_7	7500	116	7500*116=870000
A_{12}	3000	116	3000*116=348000
A_{13}	20000	116	20000*116=23200000

Residual Vulnerability Security Risk:

For V_1: 6+5+4+5+7=27

For V_2: 5+5+7+4+3=24

For V_5: 6+5+3+4+4=22

For V_8: 4+5+6+3+3=21

For V_9: 4+4+4+6+4=22

Substitute the above values accordingly

Risk due to V_1= [(400000*27) + (200000*27) + (210000*40) + (7500*27) + (3000*27) + (20000*27)]/100 =226935

Risk due to V_2= [(400000*24) + (200000*24) + (210000*24) + (7500*24) + (3000*24) + (20000*24)]/100 =201720

Risk due to V_5= [(400000*22) + (200000*22) + (210000*22) + (7500*22) + (3000*22) + (20000*22)]/100=184910

Risk due to V_8= [(400000*21) + (200000*21) + (210000*21) + (7500*21) + (3000*21) + (20000*21)]/100=176505

Risk due to V_9= [(400000*22) + (200000*22) + (210000*22) + (7500*22) + (3000*22) + (20000*22)]/100=184910

Ranking of residual asset risk:

ASSET	–	RESIDUAL RISK	-	RANK
A_1	-	46400000	-	1
A_6	-	24360000	-	2
A_2	-	23200000	-	3
A_{13}	-	23200000	-	4
A_7	-	870000	-	5
A_{12}	-	348000	-	6

Ranking of residual vulnerability security risk:

VULNERABILITY	–	RESIDUAL RISK	-	RANK
V_1	-	226935	-	1
V_2	-	201720	-	2
V_5	-	184910	-	3
V_9	-	184910	-	4
V_8	-	176505	-	5

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

There have been MOT controls that have not been implemented and followed to the full potential like backing up data every night, securing data, especially payroll data from unauthorized access, and modification. To enhance the security of HGA, the CISO has proposed the installation of assets like DMZ and VPN which facilitate secure communication over a network. And also, the installation of firewalls and computer packages to protect against viruses would also assist in securing the confidentiality, integrity, and availability of resources of the agency. The focus should be laid on timely monitoring how various security measures proposed are being followed and if there's any measure that needs to be updated to provide an extra level of security according to the ongoing risk situation, it has to be immediately reported to the concerned risk management team to avoid worsening of scenario.

Security Risk Response (Resilience) Strategy Step R1: Start with the results derived in Step P3 above. Keep threat/vulnerability pairs with probabilities as calculated in Step P3. Then calculate updated Residual Risk Rankings and Vulnerability Risk Rankings due to reducing risk impacts to less than 100% based on implementing M-O-T controls which reduce risk impacts.

Management	Operational	Technical
Computer system policies employed and followed are inclined towards payroll data security-related issues. (MOT$_{1)}$	Restrictions on sharing of credentials. (MOT$_{3)}$	Automated access control to decrease unauthorized access and corruption of time and attendance data accidentally. (MOT$_{7)}$
Managing the accessibility of data based on its type and confidentiality. (MOT$_{2)}$	Mandatory security awareness training or live interactive course for new employees. (MOT$_{4)}$	Application on the LAN server that checks the correctness and validity of the time and attendance data. (MOT$_{8)}$
	Backup of time and attendance data. (MOT$_{5)}$	Authorized system administrators are allowed to install COG approved licensed, copyrighted packages for PC to protect them from viruses. (MOT$_{9)}$
	Develop and test contingency plans annually to discover individuals and resources needed to ensure the continuity of organizations' operations. (MOT$_{6)}$	Traffic is filtered and managed on the network by the use of firewall. (MOT$_{10}$).
	Encryption of data sent and received to the LAN hardware	

	to protect against intruders. (MOT11).	

On following the process for the remaining vulnerabilities, we get the final threat-vulnerability pairs as shown below:

	T_1	T_2	T_5	T_7	T_9
V_1	4	5	3	2	2
V_2	2	3	5	1	1
V_5	5	2	3	2	1
V_8	4	5	2	3	2
V_9	1	4	3	4	2

	Threat X Vulnerability – threat exploiting the vulnerability															
ASSETS	T_1* V_1	T_1* V_2	T_1* V_5	T_1* V_8	T_1* V_9	T_2* V_1	T_2* V_2	T_2* V_5	T_2* V_8	T_2* V_9	T_5* V_1	T_5* V_2	T_5* V_5	T_5* V_8	T_5* V_9	T_7* V_1
A_1	40%	50%	30%	50%	40%	20%	50%	50%	30%	30%	40%	20%	50%	40%	30%	30%
A_2	50%	20%	30%	30%	50%	30%	40%	20%	50%	50%	40%	30%	20%	50%	50%	50%
A_6	50%	30%	50%	20%	40%	30%	20%	50%	40%	30%	30%	20%	40%	40%	50%	20%
A_7	40%	50%	30%	50%	40%	20%	50%	50%	30%	30%	40%	20%	50%	40%	30%	30%
A_{12}	50%	30%	20%	20%	40%	30%	20%	20%	40%	30%	30%	20%	40%	40%	30%	20%
A_{13}	50%	20%	30%	30%	50%	30%	40%	20%	50%	50%	40%	30%	20%	50%	50%	50%

	Threat X Vulnerability – threat exploiting the vulnerability								
ASSETS	T_7*V_2	T_7*V_5	T_7*V_8	T_7*V_9	T_9*V_1	T_9*V_2	T_9*V_5	T_9*V_8	T_9*V_9
A_1	30%	50%	20%	20%	40%	50%	40%	20%	30%
A_2	50%	50%	40%	40%	20%	30%	30%	50%	40%
A_6	40%	30%	40%	50%	30%	20%	20%	50%	30%
A_7	30%	50%	20%	20%	40%	50%	40%	20%	30%
A_{12}	50%	50%	40%	50%	20%	20%	30%	40%	40%
A_{13}	50%	50%	40%	40%	20%	30%	30%	50%	40%

Residual asset security risk:

1) Asset A_1:-
= 400000 * [(4*40) + (2*50) + (5*30) + (4*50) + (1*40) + (5*20) + (3*50) + (2*50) + (5*30) + (4*30) + (3*40) + (5*20) + (3*50) + (2*40) + (3*30) + (2*30) + (1*30) + (2*50) + (3*20) + (4*20) + (2*40) + (1*50) + (1*40) + (2*20) + (2*30)] / 10000
= 96400

2) Asset A_2:-
= 200000 * [(4*50) + (2*20) + (5*30) + (4*30) + (1*50) + (5*30) + (3*40) + (2*20) + (5*50) + (4*50) + (3*40) + (5*30) + (3*20) + (2*50) + (3*50) + (2*50) + (1*50) + (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)] / 10000
= 54200

3) Asset A_6:-
= 210000 * [(4*50) + (2*30) + (5*50) + (4*20) + (1*40) + (5*30) + (3*20) + (2*50) + (5*40) + (4*30) + (3*30) + (5*20) + (3*40) + (2*40) + (3*50) + (2*20) + (1*40) + (2*30) + (3*40) + (4*50) + (2*30) + (1*20) + (1*20) + (2*50) + (2*30)]/ 10000
= 52920

4) Asset A_7:-
= 7500 * [(4*40) + (2*50) + (5*30) + (4*50) + (1*40) + (5*20) + (3*50) + (2*50) + (5*30) + (4*30) + (3*40) + (5*20) + (3*50) + (2*40) + (3*30) + (2*30) + (1*30) + (2*50) + (3*20) + (4*20) + (2*40) + (1*50) + (1*40) + (2*20) + (2*30)] / 10000
= 1807.5

5) Asset A_{12}:-
= 3000 * [(4*50) + (2*30) + (5*20) + (4*20) + (1*40) + (5*30) + (3*20) + (2*20) + (5*40) + (4*30) + (3*30) + (5*20) + (3*40) + (2*40) + (3*30) + (2*20) + (1*50) + (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)] / 10000
= 684

6) Asset A_{13}:-
= 20000 * [(4*50) + (2*20) + (5*30) + (4*30) + (1*50) + (5*30) + (3*40) + (2*20) + (5*50) + (4*50) + (3*40) + (5*30) + (3*20) + (2*50) + (3*50) + (2*50) + (1*50) + (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)] / 10000
= 5420

Residual vulnerability security risk:

1) Risk due to V_1:-
=(1/10000)*[400000 * [4*40+5*20+3*40+2*30+2*40] + 200000 * [4*50+5*30+3*40+2*50+2*20] + 210000 * [4*50+5*30+3*30+2*20+2*30] + 7500* [4*40+5*20+3*40+2*30+2*40]+ 3000 * [4*50+5*30+3*30+2*20+2*20] + 20000* [4*50+5*30+3*40+2*50+2*20]= 46106

2) Risk due to V_2:-
= 400000 * [2*50+3*50+5*20+1*30+1*50] + 200000 * [2*20+3*40+5*30+1*50+1*30] + 210000 * [2*30+3*20+5*20+1*40+1*20] + 7500* [2*50+3*50+5*20+1*30+1*50] + 3000 * [2*30+3*20+5*20+1*50+1*30] + 20000* [2*20+3*40+5*30+1*50+1*30] = 32072.5

3) Risk due to V_5:-
= 400000 * [5*30+2*50+3*50+2*50+1*40] + 200000 * [5*30+2*20+3*20+2*50+1*30] + 210000 * [5*50+2*50+3*40+2*30+1*20] + 7500* [5*30+2*50+3*50+2*50+1*40] + 3000 * [5*20+2*20+3*40+2*50+1*30] + 20000* [5*30+2*20+3*20+2*50+1*30] = 42032

4) Risk due to V_8:-
= 400000 * [4*50+5*30+2*40+3*20+2*20] + 200000 * [5*30+2*50+3*50+2*40+1*50] + 210000 * [5*20+2*40+3*40+2*40+1*50] +

7500* [4*50+5*30+2*40+3*20+2*20] + 3000 * [5*20+2*40+3*40+2*40+1*50] + 20000* [5*30+2*50+3*50+2*40+1*50] = 42416.5

5) Risk due to V_9:-
= 400000 * [1*40+4*30+3*30+4*20+2*30] + 200000 * [5*50+2*50+3*50+2*40+1*40] + 210000 * [5*40+2*30+3*50+2*50+1*30] + 7500* [1*40+4*30+3*30+4*20+2*30] + 3000 * [5*40+2*30+3*30+2*40+1*40] + 20000* [5*50+2*50+3*50+2*40+1*40] = 41013.5

Ranking of residual asset risk:

ASSET	RESIDUAL RISK	RANK
A_1	96400	1
A_2	54200	2
A_6	52920	3
A_7	1807.5	4
A_{12}	684	5
A_{13}	482	6

Ranking of residual vulnerability security risk:

VULNERABILITY	RESIDUAL RISK	RANK
V_1	46106	1
V_5	42032	2
V_9	41013.5	3
V_2	32072.5	4
V_8	4241.65	5

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

	T_1	T_2	T_5	T_7	T_9
V_1	4	5	3	2	2
V_2	2	3	5	1	1
V_5	5	2	3	2	1
V_8	4	5	2	3	2
V_9	1	4	3	4	2

Highest Ranked asset from R1 is *A_1*

	Threat X Vulnerability – threat exploiting the vulnerability															
ASSETS	T_1*V_1	T_1*V_2	T_1*V_5	T_1*V_8	T_1*V_9	T_2*V_1	T_2*V_2	T_2*V_5	T_2*V_8	T_2*V_9	T_5*V_1	T_5*V_2	T_5*V_5	T_5*V_8	T_5*V_9	T_7*V_1
A_1	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_2	50%	20%	30%	30%	50%	30%	40%	20%	50%	50%	40%	30%	20%	50%	50%	50%
A_6	50%	30%	50%	20%	40%	30%	20%	50%	40%	30%	30%	20%	40%	40%	50%	20%
A_7	40%	50%	30%	50%	40%	20%	50%	50%	30%	30%	40%	20%	50%	40%	30%	30%
A_{12}	50%	30%	20%	20%	40%	30%	20%	20%	40%	30%	30%	20%	40%	40%	30%	20%
A_{13}	50%	20%	30%	30%	50%	30%	40%	20%	50%	50%	40%	30%	20%	50%	50%	50%

	Threat X Vulnerability – threat exploiting the vulnerability								
ASSETS	T_7*V_2	T_7*V_5	T_7*V_8	T_7*V_9	T_9*V_1	T_9*V_2	T_9*V_5	T_9*V_8	T_9*V_9
A_1	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_2	50%	50%	40%	40%	20%	30%	30%	50%	40%
A_6	40%	30%	40%	50%	30%	20%	20%	50%	30%
A_7	30%	50%	20%	20%	40%	50%	40%	20%	30%
A_{12}	50%	50%	40%	50%	20%	20%	30%	40%	40%
A_{13}	50%	50%	40%	40%	20%	30%	30%	50%	40%

Residual asset security risk:

1) Asset A_1:-
= 400000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)] /10000
= 19200

2) Asset A_2:-
= 200000 * [(4*50) + (2*20) + (5*30) + (4*30) + (1*50) + (5*30) + (3*40) + (2*20) + (5*50) + (4*50) + (3*40) + (5*30) + (3*20) + (2*50) + (3*50) + (2*50) + (1*50) + (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)] / 10000
= 54200

3) Asset A_6:-
= 210000 * [(4*50) + (2*30) + (5*50) + (4*20) + (1*40) + (5*30) + (3*20) + (2*50) + (5*40) + (4*30) + (3*30) + (5*20) + (3*40) + (2*40) + (3*50) + (2*20) + (1*40) + (2*30) + (3*40) + (4*50) + (2*30) + (1*20) + (1*20) + (2*50) + (2*30)] / 10000
= 52920

4) Asset A_7:-
= 7500 * [(4*40) + (2*50) + (5*30) + (4*50) + (1*40) + (5*20) + (3*50) + (2*50) + (5*30) + (4*30) + (3*40) + (5*20) + (3*50) + (2*40) + (3*30) + (2*30) + (1*30) + (2*50) + (3*20) + (4*20) + (2*40) + (1*50) + (1*40) + (2*20) + (2*30)] / 10000
= 1807.5

5) Asset A_{12}:-
= 3000 * [(4*50) + (2*30) + (5*20) + (4*20) + (1*40) + (5*30) + (3*20) + (2*20) + (5*40) + (4*30) + (3*30) + (5*20) + (3*40) + (2*40) + (3*30) + (2*20) + (1*50) + (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)] / 10000
= 684

6) Asset A_{13}:-
= 20000 * [(4*50) + (2*20) + (5*30) + (4*30) + (1*50) + (5*30) + (3*40) + (2*20) + (5*50) + (4*50) + (3*40) + (5*30) + (3*20) + (2*50) + (3*50) + (2*50) + (1*50)

+ (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)] / 10000
= 5420

Residual vulnerability security risk:

1) Risk due to V_1:-
= 400000 * [4*5+5*5+3*5+2*5+2*5] + 200000 * [4*50+5*30+3*40+2*50+2*20] + 210000 * [4*50+5*30+3*30+2*20+2*30] + 7500* [4*40+5*20+3*40+2*30+2*40]+ 3000 * [4*50+5*30+3*30+2*20+2*20] + 20000* [4*50+5*30+3*40+2*50+2*20] = 28506

2) Risk due to V_2:-
= 400000 * [2*5+3*5+5*5+1*5+1*5] + 200000 * [2*20+3*40+5*30+1*50+1*30] + 210000 * [2*30+3*20+5*20+1*40+1*20] + 7500* [2*50+3*50+5*20+1*30+1*50] + 3000 * [2*30+3*20+5*20+1*50+1*30] + 20000* [2*20+3*40+5*30+1*50+1*30] = 17272.5

3) Risk due to V_5:-
= 400000 * [5*5+2*5+3*5+2*5+1*5] + 200000 * [5*30+2*20+3*20+2*50+1*30] + 210000 * [5*50+2*50+3*40+2*30+1*20] + 7500* [5*30+2*50+3*50+2*50+1*40] + 3000 * [5*20+2*20+3*40+2*50+1*30] + 20000* [5*30+2*20+3*20+2*50+1*30] = 23032

4) Risk due to V_8:-
= 400000 * [4*5+5*5+2*5+3*5+2*5] + 200000 * [5*30+2*50+3*50+2*40+1*50] + 210000 * [5*20+2*40+3*40+2*40+1*50] + 7500* [4*50+5*30+2*40+3*20+2*20] + 3000 * [5*20+2*40+3*40+2*40+1*50] + 20000* [5*30+2*50+3*50+2*40+1*50] = 24416.5

5) Risk due to V_9:-
= 400000 * [1*5+4*5+3*5+4*5+2*5] + 200000 * [5*50+2*50+3*50+2*40+1*40] + 210000 * [5*40+2*30+3*50+2*50+1*30] + 7500* [1*40+4*30+3*30+4*20+2*30] + 3000 * [5*40+2*30+3*30+2*40+1*40] + 20000* [5*50+2*50+3*50+2*40+1*40] = 28213.5

Ranking of residual asset risk:

ASSET	– RESIDUAL RISK	- RANK
A_2 -	54200	- 1
A_6 -	52920	- 2
A_1 -	19200	- 3
A_7 -	1807.5	- 4
A_{12} -	684	- 5
A_{13} -	482	- 6

Ranking of residual vulnerability security risk:

VULNERABILITY	– RESIDUAL RISK	- RANK
V_1 -	28506	- 1
V_9 -	28213.5	- 2
V_8 -	24416.5	- 3
V_5 -	23032	- 4
V_2 -	17272.5	- 5

Security Risk Response (Resilience) Strategy Step R3: Apply additional Hardening Controls to new now highest ranked Residual Asset Risk, thus reducing risk impact probabilities, further reducing the overall security asset residual risk, and creating a new ranking of vulnerability security risks. In this step, you need to include the value of points from the Hardening Controls in Step R2 in the Asset inventory (!) and increase asset risk loss (for example by restriction of services impacting operational effectiveness or possibly total loss of the asset, but not the service, that has a redundant back-up).

	T_1	T_2	T_5	T_7	T_9
V_1	4	5	3	2	2
V_2	2	3	5	1	1
V_5	5	2	3	2	1
V_8	4	5	2	3	2
V_9	1	4	3	4	2

Highest Ranked asset from R1 is *A_2*

	Threat X Vulnerability – threat exploiting the vulnerability															
ASSETS	T_1*V_1	T_1*V_2	T_1*V_5	T_1*V_8	T_1*V_9	T_2*V_1	T_2*V_2	T_2*V_5	T_2*V_8	T_2*V_9	T_5*V_1	T_5*V_2	T_5*V_5	T_5*V_8	T_5*V_9	T_7*V_1
A_1	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_2	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_6	50%	30%	50%	20%	40%	30%	20%	50%	40%	30%	30%	20%	40%	40%	50%	20%
A_7	40%	50%	30%	50%	40%	20%	50%	50%	30%	30%	40%	20%	50%	40%	30%	30%
A_{12}	50%	30%	20%	20%	40%	30%	20%	20%	40%	30%	30%	20%	40%	40%	30%	20%
A_{13}	50%	20%	30%	30%	50%	30%	40%	20%	50%	50%	40%	30%	20%	50%	50%	50%

	Threat X Vulnerability – threat exploiting the vulnerability								
ASSETS	T_7*V_2	T_7*V_5	T_7*V_8	T_7*V_9	T_9*V_1	T_9*V_2	T_9*V_5	T_9*V_8	T_9*V_9
A_1	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_2	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_6	40%	30%	40%	50%	30%	20%	20%	50%	30%
A_7	30%	50%	20%	20%	40%	50%	40%	20%	30%
A_{12}	50%	50%	40%	50%	20%	20%	30%	40%	40%
A_{13}	50%	50%	40%	40%	20%	30%	30%	50%	40%

Residual asset security risk:

1) Asset A_1:-
= 400000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]
= 19200

2) Asset A_2:-
= 200000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]
= 9600

3) Asset A_6:-
= 210000 * [(4*50) + (2*30) + (5*50) + (4*20) + (1*40) + (5*30) + (3*20) + (2*50) + (5*40) + (4*30) + (3*30) + (5*20) + (3*40) + (2*40) + (3*50) + (2*20) + (1*40) + (2*30) + (3*40) + (4*50) + (2*30) + (1*20) + (1*20) + (2*50) + (2*30)]
= 52920

4) Asset A_7:-
= 7500 * [(4*40) + (2*50) + (5*30) + (4*50) + (1*40) + (5*20) + (3*50) + (2*50) + (5*30) + (4*30) + (3*40) + (5*20) + (3*50) + (2*40) + (3*30) + (2*30) + (1*30) + (2*50) + (3*20) + (4*20) + (2*40) + (1*50) + (1*40) + (2*20) + (2*30)]
= 1807.5

5) Asset A_{12}:-
= 3000 * [(4*50) + (2*30) + (5*20) + (4*20) + (1*40) + (5*30) + (3*20) + (2*20) + (5*40) + (4*30) + (3*30) + (5*20) + (3*40) + (2*40) + (3*30) + (2*20) + (1*50) + (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)]
= 684

6) Asset A_{13}:-
= 20000 * [(4*50) + (2*20) + (5*30) + (4*30) + (1*50) + (5*30) + (3*40) + (2*20) + (5*50) + (4*50) + (3*40) + (5*30) + (3*20) + (2*50) + (3*50) + (2*50) + (1*50) + (2*50) + (3*40) + (4*40) + (2*20) + (1*30) + (1*30) + (2*50) + (2*40)]
= 482

Residual vulnerability security risk:

1) Risk due to V_1:-
= 400000 * [4*5+5*5+3*5+2*5+2*5] + 200000 * [4*5+5*5+3*5+2*5+2*5] + 210000 * [4*50+5*30+3*30+2*20+2*30] + 7500* [4*40+5*20+3*40+2*30+2*40]+ 3000 * [4*50+5*30+3*30+2*20+2*20] + 20000* [4*50+5*30+3*40+2*50+2*20] = 17906

2) Risk due to V_2:-
= 400000 * [2*5+3*5+5*5+1*5+1*5] + 200000 * [2*5+3*5+5*5+1*5+1*5] + 210000 * [2*30+3*20+5*20+1*40+1*20] + 7500* [2*50+3*50+5*20+1*30+1*50] + 3000 * [2*30+3*20+5*20+1*50+1*30] + 20000* [2*20+3*40+5*30+1*50+1*30] = 10672.5

3) Risk due to V_5:-
= 400000 * [5*5+2*5+3*5+2*5+1*5] + 200000 * [5*5+2*5+3*5+2*5+1*5] + 210000 * [5*50+2*50+3*40+2*30+1*20] + 7500* [5*30+2*50+3*50+2*50+1*40] + 3000 * [5*20+2*20+3*40+2*50+1*30] + 20000* [5*30+2*20+3*20+2*50+1*30] = 16732

4) Risk due to V_8:-
= 400000 * [4*5+5*5+2*5+3*5+2*5] + 200000 * [4*5+5*5+2*5+3*5+2*5] + 210000 * [4*20+5*40+2*40+3*40+2*50] + 7500* [4*50+5*30+2*40+3*20+2*20] + 3000 * [4*20+5*40+2*40+3*40+2*50] + 20000* [4*30+5*50+2*50+3*40+2*50] = 18931.5

5) Risk due to V_9:-
= 400000 * [1*5+4*5+3*5+4*5+2*5] + 200000 * [1*5+4*5+3*5+4*5+2*5] + 210000 * [1*40+4*30+3*50+4*50+2*30] + 7500* [1*40+4*30+3*30+4*20+2*30] + 3000 * [1*40+4*30+3*30+4*40+2*40] + 20000* [1*50+4*50+3*50+4*40+2*40] = 17889.5

Ranking of residual asset risk:

ASSET –	RESIDUAL RISK -	RANK
A_6 -	52920	- 1
A_1 -	19200	- 2
A_2 -	9600	- 3
A_7 -	1807.5	- 4
A_{12} -	684	- 5
A_{13} -	482	- 6

Ranking of residual vulnerability security risk:

VULNERABILITY –	RESIDUAL RISK -	RANK
V_8 -	18931.5	- 1
V_1 -	17906	- 2
V_9 -	17889.5	- 3

V_5	-	15116.5	-	4
V_2	-	10672.5	-	5

Mixed Strategy: Include all necessary new controls by combining Steps P3 and R3.

On considering and following the new security controls, a reduction in the probabilities is observed.

	T_1	T_2	T_5	T_7	T_9
V_1	4	5	3	2	2
V_2	2	3	5	1	1
V_5	5	2	3	2	1
V_8	4	5	2	3	2
V_9	1	4	3	4	2

	Threat X Vulnerability – threat exploiting the vulnerability															
ASSETS	T_1*V_1	T_1*V_2	T_1*V_5	T_1*V_8	T_1*V_9	T_2*V_1	T_2*V_2	T_2*V_5	T_2*V_8	T_2*V_9	T_5*V_1	T_5*V_2	T_5*V_5	T_5*V_8	T_5*V_9	T_7*V_1
A_1	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_2	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_6	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_7	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_{12}	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_{13}	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%	5%

	Threat X Vulnerability – threat exploiting the vulnerability								
ASSETS	T_7*V_2	T_7*V_5	T_7*V_8	T_7*V_9	T_9*V_1	T_9*V_2	T_9*V_5	T_9*V_8	T_9*V_9
A_1	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_2	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_6	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_7	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_{12}	5%	5%	5%	5%	5%	5%	5%	5%	5%
A_{13}	5%	5%	5%	5%	5%	5%	5%	5%	5%

Residual asset security risk:

1) Asset A_1:-

   = 400000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]

   = 19200

2) Asset A_2:-

   = 200000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]

   = 9600

3) Asset A_6:-

   = 210000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]

   = 10080

4) Asset A_7:-

   = 7500 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]

   = 360

5) Asset A_{12}:-

   = 3000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]

   = 144

6) Asset A_{13}:-

   = 20000 * [(4*5) + (2*5) + (5*5) + (4*5) + (1*5) + (5*5) + (3*5) + (2*5) + (5*30) + (4*5) + (3*5) + (5*5) + (3*5) + (2*5) + (3*5) + (2*5) + (1*5) + (2*5) + (3*5) + (4*5) + (2*5) + (1*5) + (1*5) + (2*5) + (2*5)]

   = 960

Residual vulnerability security risk:

1) Risk due to V_1:-
= 400000 * [4*5+5*5+3*5+2*5+2*5] + 200000 * [4*5+5*5+3*5+2*5+2*5] + 210000 * [4*5+5*5+3*5+2*5+2*5] + 7500* [4*5+5*5+3*5+2*5+2*5] + 3000 * [4*5+5*5+3*5+2*5+2*5] + 20000* [4*5+5*5+3*5+2*5+2*5]
= 6724

2) Risk due to V_2:-
= 400000 * [2*5+3*5+5*5+1*5+1*5] + 200000 * [2*5+3*5+5*5+1*5+1*5] + 210000 * [2*5+3*5+5*5+1*5+1*5] + 7500 * [2*5+3*5+5*5+1*5+1*5] + 3000 * [2*5+3*5+5*5+1*5+1*5] + 20000 * [2*5+3*5+5*5+1*5+1*5]
= 5043

3) Risk due to V_5:-
= 400000 * [5*5+2*5+3*5+2*5+1*5] + 200000 * [5*5+2*5+3*5+2*5+1*5] + 210000 * [5*5+2*5+3*5+2*5+1*5] + 7500* [5*5+2*5+3*5+2*5+1*5] + 3000 * [5*5+2*5+3*5+2*5+1*5] + 20000* [5*5+2*5+3*5+2*5+1*5]
= 5463.25

4) Risk due to V_8:-
= 400000 * [4*5+5*5+2*5+3*5+2*5] + 200000 * [4*5+5*5+2*5+3*5+2*5] + 210000 * [4*5+5*5+2*5+3*5+2*5] + 7500* [4*5+5*5+2*5+3*5+2*5] + 3000 * [4*5+5*5+2*5+3*5+2*5] + 20000* [4*5+5*5+2*5+3*5+2*5]
= 6424

5) Risk due to V_9:-
= 400000 * [1*5+4*5+3*5+4*5+2*5] + 200000 * [1*5+4*5+3*5+4*5+2*5] + 210000 * [1*5+4*5+3*5+4*5+2*5] + 7500 * [1*5+4*5+3*5+4*5+2*5] + 3000 * [1*5+4*5+3*5+4*5+2*5] + 20000 * [1*5+4*5+3*5+4*5+2*5]
= 5883.5

Ranking of residual asset risk:

ASSET –	RESIDUAL RISK -	RANK
A_1 -	19200	- 1
A_6 -	10080	- 2
A_2 -	9600	- 3
A_{13} -	9600	- 4

A_7	360	5
A_{12}	144	6

Ranking of residual vulnerability security risk:

VULNERABILITY	RESIDUAL RISK	RANK
V_1	6724	1
V_8	6424	2
V_9	5883.5	3
V_5	5463.25	4
V_2	5043	5

Conclusion

Cost-benefit analysis

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

In the process of making a risk assessment of HGA, as an initial step, the list of all the assets with their asset values and explanation, the vulnerabilities of the assets, and the possible threats that might occur are also listed. The various risk prevention strategies are performed and the vulnerabilities and assets are ranked according to the severity of an occurrence of the risk. The asset ranking depicts the probability of an asset being susceptible to risk. The vulnerability ranking ranks the vulnerabilities in the rank of their probability of severity and occurrence. Both, qualitative and quantitative analysis of risk is performed to show the value of assets in terms of probability terms like High, Medium, Low, and also in USD.

The ranking of the assets and vulnerabilities is done on the basis of residual risk. Residual risk can be defined as the risk that is remaining after various security measures, strategies and controls have been applied to mitigate risk.

The risk prevention strategy refers to all the techniques and measures used to prevent the occurrence of the risk. It can be inferred from the above that with the application of each security prevention strategy, the probability of assets being exposed to threats and the residual risk caused due to each asset is reducing gradually. And also, a reduction in the residual vulnerability security risk can be observed.

As there can be risks that cannot be prevented. Like in certain scenarios, risks can be unavoidable, then the risk response strategies are enforced. A risk response strategy refers to the methods that are used to reduce the impact of risk once it has occurred. Basically, it is done in response to a risk occurrence. By analyzing the above strategies, it can be inferred that the residual risk due to vulnerabilities and assets has decreased more and has come to a very low stage.

HGA has implemented various MOT controls completely such as verifying the integrity of data, training the new employees on the security of the company. These security controls focus on securing the data from intruders or unauthorized people, making all the employees aware of the security policies of the agency so that they can deal with scenarios of risk. But there are certain areas of the agency's security that had to be addressed by enforcing new security controls such as the use of digital signatures, regularly monitoring the audit logs is also very important as it will give a prior view of any future risk scenario, faster installation of applications or software that fix bugs. And as the new security controls were in accordance with the federal government, they can also handle any risk scenarios that probably might be unknown to HGA but known to the risk management and assessment teams in central government. Hence HGA will be well in advance prepared for any situation as it has to deal with the distribution of funds from the government to individuals. As it is associated with some operations with the government, enforcing controls and strategies for security is crucial.

Hence a combination of the existing security controls and the newly proposed controls will enhance the security of the agency and will protect the confidentiality, integrity, and availability of the resources of the agency.

Now compare Risk Prevention and Risk Response strategies. Do you recommend a Risk Prevention Strategy, a Risk Response Strategy, or a mixed strategy as a combination of both? Explain clearly your analysis and recommendations.

Risk prevention strategy aims at finding the individuals or assets of a firm that could have vulnerabilities that can be exploited to further result in a situation of threat to the company. Risk response strategy implies the measures or steps that need to be done after an exploit or breach of data or resources of the firm has occurred. It means the reaction strategies for such situations of data exploit.

I opine that a mixed strategy consisting of a combination of both would be ideal. Every threat that would occur can be prevented by many measures. Measures also require being attentive to happenings in the organizations, the state of various resources and data present, etc. This does suffice the purpose of threat prevention but not always. As it employs a lot of human effort, time, and cost from company management, scenarios can arise where the act of monitoring the company's security would be performed in a hurry or ignored completely. In such cases, there's a high likelihood that a threat can occur. In such instances, the company has to apply a risk response strategy.

Therefore I recommend having a mixed strategy that would present the various risk prevention and risk response strategy.

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

Controls mitigating	**Risk prevention budget**	**Risk response budget**	**Mixed strategy budget**
Payroll fraud	$70000	$67000	$130000
Payroll errors	$80000	$87000	$105000
Continuation of operations	$67000	$70000	$160000
Sensitive information disclosure	$88000	$80000	$150000
Network related attacks	$59000	$63000	$120000
Review of security controls	$50000	$46000	$76000
VPN	$8000	$16000	$45000
DMZ	$10000	$15000	$50000
TOTAL	**549000**	**554000**	**1107000**

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

= 840500 – 48984 = 791516

The value of risk exceeds the budget.

Proposed security risk budget Cost:

1) Cost-benefit ratio analysis for risk prevention budget

= Proposed risk security budget cost / expected security risk benefit

= 549000 / 48984

= 11.20

2) Cost-benefit ratio analysis for risk response budget

= Proposed risk security budget cost / expected security risk benefit

= 554000 / 48984

= 11.30

3) Cost-benefit ratio analysis for mixed budget

= Proposed risk security budget cost / expected security risk benefit

= 1107000 / 48984

= 22.59

PART B) SECURITY RISK MANAGEMENT IMPLEMENTATION PLAN

Access control security risk management implementation controls and policies:

1. Identification controls:
2. Personal authentication:
3. Authorization
4. Logical access control methods:
5. Physical access control methods:
6. Biometric systems:

A list of critical assets:

ASSET ID	ASSET NAME	VALUE IN $
A_1	Personal identifiable information	$500000
A_2	Financial resources	$550000
A_3	Server	$350000
A_4	Database	$450000
A_5	Laptops and desktops	$550000
A_6	Trust	Intangible asset
A_7	Reputation	Intangible asset

List of missing controls:

1. Digital certificate
2. Asset safety
3. Biometric manipulation
4. Security questions
5. ID Card and badges

List of potential vulnerabilities:

1. Unauthorized access
2. Social engineering
3. Theft
4. Absence of encryption techniques
5. Unauthorized modification

List of potential threats:

1. Modification of data
2. Loss of sensitivity to information
3. Loss of ID Card and badges
4. Loss of information
5. Loss of data integrity

6. Sniffing of traffic and information

List of potential risks:

1. Loss of integrity and unauthorized viewing of data during transfer across a network
2. Loss of data and unauthorized modification due to improper security standards. Disclosure and selling of sensitive information.
3. Tampering of biometric information to get access to resources and rooms.
4. Absence of the second authentication process due to which any intruder with credentials can log in and access the employee portal.
5. Social engineering can be used to get answers to security questions and illegally access the employee portal.
6. Loss of ID Card and badges due to theft paves way for unauthorized access to assets, resources, and rooms.
7. Unauthorized modification of scanner strip
8. Social engineering is used to get ID Card and badges.

Network infrastructure security risk management implementation controls and policies:

1. Enclave protection
2. Firewalls
3. routers

A list of critical assets:

ASSET ID	ASSET NAME	VALUE IN $
A_1	Personal identifiable information	$500000
A_2	Financial resources	$550000
A_3	Server	$350000
A_4	Database	$450000
A_5	Laptops and desktops	$550000
A_6	Trust	Intangible asset
A_7	Reputation	Intangible asset

List of missing controls:

1. Demilitarised zone
2. Test access point
3. Stateful inspection firewall

4. Bastion host

List of potential vulnerabilities:

1. Unauthorized access
2. Wireless attack
3. Theft
4. Disclosure of sensitive information

List of potential threats:

1. Modification of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of data integrity
5. Loss of information

List of potential risks:

1. Modification of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of information
5. Unauthorized access
6. Degradation of system immunity to resist attacks
7. Malware intrusion
8. Allowing untrusted or malicious traffic

Network infrastructure security risk management implementation controls and policies:

1. Ports, protocols, and services
2. Device management
3. Device monitoring
4. Network authentication, authorization, and accounting
5. NIDS
6. Switches and VLANs
7. Virtual Private Network

A list of critical assets:

ASSET ID	ASSET NAME	VALUE IN $
A_1	Personal identifiable information	$500000

A_2	Financial resources	$550000
A_3	Server	$350000
A_4	Database	$450000
A_5	Laptops and desktops	$550000
A_6	Trust	Intangible asset
A_7	Reputation	Intangible asset

List of missing controls:

1. Unicast reverse path forwarding
2. Router password protection
3. VLAN trunking
4. Host to host

List of potential vulnerabilities:

1. Unauthorized access
2. Dropping or loss of packets
3. IP address spoofing
4. Unsecure wireless network
5. MITM attack
6. Trojans and worms

List of potential threats:

1. Modification of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of data integrity
5. Loss of information
6. Deletion of files

List of potential risks:

1. Modification of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of information
5. Unauthorized access
6. Sabotage communication
7. Malware intrusion
8. MITM attack
9. DNS hijacking

Database security risk management implementation controls and policies:

1. Authentication
2. Authorization
3. Confidentiality
4. Data integrity
5. Auditing
6. Replication and Federation
7. Clustering
8. Backup and recovery
9. Operating system authorization
10. Application protection
11. Network protection
12. Security design and configuration
13. Enclave computing environment
14. Business continuity
15. Vulnerability and incident management

A list of critical assets:

ASSET ID	ASSET NAME	VALUE IN $
A_1	Personal identifiable information	$500000
A_2	Financial resources	$550000
A_3	Server	$350000
A_4	Database	$450000
A_5	Laptops and desktops	$550000
A_6	Trust	Intangible asset
A_7	Reputation	Intangible asset

List of missing controls:

1. Database auditor
2. External authentication
3. Renaming default accounts
4. Time and count time limits
5. Trusted recovery

List of potential vulnerabilities:

1. Unauthorized access
2. Information theft
3. DDOS attack
4. Session hijacking
5. Loss of data

List of potential threats:

1. Modification and access of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of data integrity
5. Loss of data

List of potential risks:

1. Modification of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of information
5. Unauthorized access
6. Sabotage communication
7. MITM attack
8. Session hijacking
9. Trojan and malware
10. Lack of sufficient knowledge about database functionality

Application infrastructure security risk management implementation controls and policies:

1. Application data handling
2. Authentication
3. Cryptography
4. User accounts
5. Input validation
6. Auditing
7. Configuration management
8. Testing deployment

A list of critical assets:

ASSET ID	ASSET NAME	VALUE IN $
A_1	Personal identifiable information	$500000
A_2	Financial resources	$550000
A_3	Server	$350000
A_4	Database	$450000
A_5	Laptops and desktops	$550000
A_6	Trust	Intangible asset
A_7	Reputation	Intangible asset

List of missing controls:

1. Data marking
2. Use of message authentication code
3. Protecting audit trails
4. Automated tools

List of potential vulnerabilities:

1. Unauthorized access
2. Information theft
3. Improper modification of data
4. Improper error diagnosis
5. Database attack

List of potential threats:

1. Modification and access of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of data integrity
5. Loss of data

List of potential risks:

1. Loss of CIA triad and privacy to data
2. Loss of information
3. Unauthorized access
4. Loss of consistency and accuracy of data.
5. Malware intrusion

Wireless infrastructure security risk management implementation controls and policies:

1. Wireless WAN risk management
2. Wireless PAN Risk management
3. Wireless WAN security
4. Wireless RFID Risk management
5. Wireless PED Risk management

List of potential vulnerabilities:

1. Unauthorized access
2. Information theft
3. Network sniffing
4. MITM

List of potential threats:

1. Modification and access of data by intruders
2. Loss of sensitivity to information
3. Loss of CIA triad and privacy to data
4. Loss of data integrity
5. Loss of data

List of potential risks:

1. Loss of CIA triad and privacy to data
2. Loss of information
3. Unauthorized access
4. Loss of consistency and accuracy of data.
5. Loss of sensitivity to data
6. Loss of availability of resources

List of Cybersecurity Implementation controls that exist at InnoFirm

A) Access control security risk management implementation controls and policies:

Cybersecurity controls	
Identification controls	Employee ID Card
	Username and password
	Biometrics
	Encrypted badges
Personal authentication	Employee ID Card
	Username and password
	Digital certificate
	Biometrics
	Encrypted badges
Authorization	Regulations and policies
	Access control list
	Multifactor authentication
Logical access control methods	Network architecture controls
	Digital lock
	Password
	Digital certificate
	Biometrics
	PIN
Physical access control methods	Access points
	Access control server
	Keypads
	Control panel
	Intrusion detection techniques
	Storage and handling
Biometric systems	Fingerprint scanner
	Iris scanner

B) Network infrastructure security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name
Enclave protection	Defence-in-depth technology
	Firewall
	Routers
	Intrusion detection system
	Intrusion prevention system
	Wireless intrusion detection system

	VPN
Firewall	Packet filtering firewall
	Deep packet inspection firewall
	Proxy servers
	Hybrid technology firewall
Router	Routing table integrity
	Securing routing planes
	ISP router

C) Network infrastructure security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name
Ports, protocols, and services	Blocking protocols on enclave perimeter
	Restricting ICMPv4 request and response messages
	Blocking trace-route
	IPv4 address filtering
	IPv6 address filtering
	Protection against SYN flood attack
Device management	Device vulnerability management system
	Out-of-band device management
	In-band device management
Device monitoring	Simple Network Management Protocol (SNMP)
	Network Management Station
Network authentication, authorization, and accounting	Authentication
	Authorization
	Accounting
	Audit logs
NIDS	External NIDS
	Internal NIDS
Switches and VLANs	Physical switches and wiring
	Virtual Local area network (VLANs)
	VLAN port-security
	VLAN 802.1x and Management Policy Server
Virtual Private Network	Gateway to gateway
	Host to gateway

D) Database security risk management implementation controls and policies

Cybersecurity implementation control type	Control name
Authentication	Employee account
	Database administrator
	Application owner
	Application user manager
	Application accounts
	Database operators
	Access control list
	Passwords
	Digital certificates
Authorization	Role-based access control
Confidentiality	Data encryption
	Encryption of application code
	Data file encryption
Data integrity	Transaction log
	Data integrity
	Audit log protection
	Audit log retention
	Audit reporting
Replication and Federation	Data replication
	Database links
Clustering	Data clustering
	Principle of least privilege
Backup and recovery	DBMS backup
	Testing and maintenance
	Authentication and authorization
Operating system authorization	Dedicated directories and files
	Dedicated operating systems account
	Updated database software
Application protection	Audit of elevated privileges
	Input validation
	authentication method
	Least privilege mechanism
Network protection	Network access
	Encrypted and protected data across a network
Security design and configuration	Procedural review
	Configuration specification
	Compliance testing
	Functional architecture for IS applications
	Non-repudiation
	Partitioning the application

	Ports, protocols, and services
	Configuration management process
	IA documentation
	System library management controls
	Security structure supports partitioning
	System state changes
	Software baseline
	Group identification and authorization
	Individual identification and authorization
	Key management
	Token and certificate standards
Enclave computing environment	Access for need-to-know
	Audit record content
	Audit trail, monitoring, analysis, and reporting
	Changes to data
	Data change controls
	Interconnection among systems and resources
	Audit of security label changes
	logon
	Privileged account control
	Marking and labeling
	Production code change controls
	Resource control
	Security configuration compliance
	Audit reduction and report generation
	Software development change controls
	Warning message
	Boundary mechanism
	Remote access for privileged functions
Business continuity	Protection of backup and restoration of assets
	Data backup procedures
	Disaster and recovery planning
	Backup copies of critical software
Vulnerability and incident management	Vulnerability management

E) Application infrastructure security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name
Application data handling	Database management system
	Data storage
	In-memory data handling
	Data transmission
	Data integrity
Authentication	Server authentication
	User authentication
	Signed code Identification
	Standalone application authentication
	Server application authentication
	Client application authentication
	Client-server application authentication
	Application component authentication
	PKI certificate validation
	Password complexity and maintenance
	Authentication credentials protection
Cryptography	Symmetric cryptography
	Use of digital signatures
User accounts	Account rules
	Account lockout policy
	Avoiding duplicate accounts
	Application sessions
	Access control
Input validation	User input validation
	Web encoding
	Race condition
	Static analysis
	Sensitive information disclosure
Auditing	Notification and audit content
Configuration management	Software Configuration management
	Limit unauthorized access
Testing	Test plans and procedures
Deployment	Documentation
	auditing

F) Wireless infrastructure security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name
Wireless WAN risk management	IEEE 802.11x Extensible authentication protocol
	EAP-Transport layer security
	Protected extensible authentication protocol
	Separation of network
	VPN
	User authentication and data encryption services
	Wi-fi protected access
	Service set identifier (SSID)
	Access point and client identification
	RSN, WRAP, CCMP protocol
Wireless PAN Risk management	Bluetooth specification
	Device-level authentication
	Data encryption
	Pairing or bonding
	Confidentiality, integrity, authentication, and authorization
	Security models and levels
	Key management
Wireless RFID Risk management	Radio-frequency identifier tag encryption
Wireless PED Risk management	Subscriber Identity module
	Wireless email
	PDA Security

Comparison of the implementation controls discussed in class with your company's existing cyber security implementation controls:

A) **Access control security risk management implementation controls and policies:**

Cybersecurity controls		Status of implementation
Identification controls	1) Employee ID Card	Present
	2) Username and password	Present
	3) Digital certificate	Absent
	4) Biometrics	Present
	5) Encrypted badges	Present
	6) SSN	Absent
Personal authentication	7) Employee ID Card	Present
	8) Username and password	Present
	9) Digital certificate	Present
	10) Biometrics	Present
	11) Encrypted badges	Present
	12) Photograph	Absent
Authorization	13) Regulations and policies	Present
	14) Access control list	Present
	15) Multifactor authentication	Present
Logical access control methods	16) Network architecture controls	Present
	17) Digital lock	Present
	18) Password	Present
	19) Digital certificate	Present
	20) Biometrics	Present
	21) Security questions	Absent
	22) PIN	Present
Physical access control methods	23) Access points	Present
	24) Access control server	Present
	25) Keypads	Present
	26) Control panel	Present
	27) Intrusion detection techniques	Present
	28) Storage and handling	Present
Biometric systems	29) Fingerprint scanner	Present
	30) Iris scanner	Present

B) Network infrastructure security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name	Status
Enclave protection	Defence-in-depth technology	Present
	Firewall	Present
	Routers	Present
	Intrusion detection system	Present
	Intrusion prevention system	Present
	Demilitarised zone	Absent
	Test access point	Absent
	Wireless intrusion detection system	Present
	VPN	Present
Firewall	Packet filtering firewall	Present
	Stateful inspection firewall	Absent
	Deep packet inspection firewall	Present
	Proxy servers	Present
	Bastion host	Absent
	Hybrid technology firewall	Present
Router	Routing table integrity	Present
	Securing routing planes	Present
	ISP router	Present

C) Network infrastructure security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name	Status
Ports, protocols, and services	Blocking protocols on enclave perimeter	Present
	Restricting ICMPv4 request and response messages	Present
	Blocking trace-route	Present
	IPv4 address filtering	Present
	IPv6 address filtering	Present
	Unicast reverse path forwarding	Absent
	Protection against SYN flood attack	Present
	Device vulnerability management system	Present

Device management	Out-of-band device management	Present
	In-band device management	Present
Device monitoring	Simple Network Management Protocol (SNMP)	Present
	Network Management Station	Present
Network authentication, authorization, and accounting	Authentication	Present
	Authorization	Present
	Accounting	Present
	Audit logs	Present
	Router password protection	Absent
NIDS	External NIDS	Present
	Internal NIDS	Present
Switches and VLANs	Physical switches and wiring	Present
	Virtual Local area network (VLANs)	Present
	VLAN trunking	Absent
	VLAN port-security	Present
	VLAN 802.1x and Management Policy Server	Present
Virtual Private Network	Gateway to gateway	Present
	Host to gateway	Present
	Host to Host	Absent

D) Database security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name	status
Authentication	Employee account	Present
	Database administrator	Present
	Application owner	Present
	Application user manager	Present
	Application accounts	Present
	Database auditor	Absent
	Database operators	Present
	Access control list	Present
	Passwords	Present
	Digital certificates	Present
	External authentication	Absent
Authorization	Role-based access control	Present
	Renaming default accounts	Absent
Confidentiality	Data encryption	Present
	Encryption of application code	Present

	Data file encryption	Present
Data integrity	Transaction log	Present
	Data integrity	Present
	Audit log protection	Present
	Audit log retention	Present
	Audit reporting	Present
Replication and Federation	Data replication	Present
	Database links	Present
Clustering	Data clustering	Present
	Principle of least privilege	Present
Backup and recovery	DBMS backup	Present
	Testing and maintenance	Present
	Authentication and authorization	Present
Operating system authorization	Dedicated directories and files	Present
	Dedicated operating systems account	Present
	Updated database software	Present
Application protection	Audit of elevated privileges	Present
	Input validation	Present
	authentication method	Present
	Least privilege mechanism	Present
Network protection	Network access	Present
	Time and count time limits	Absent
	Encrypted and protected data across a network	Present
Security design and configuration	Procedural review	Present
	Configuration specification	Present
	Compliance testing	Present
	Functional architecture for IS applications	Present
	Non-repudiation	Present
	Partitioning the application	Present
	Ports, protocols, and services	Present
	Configuration management process	Present
	IA documentation	Present
	System library management controls	Present
	Security structure supports partitioning	Present
	System state changes	Present
	Software baseline	Present

	Group identification and authorization	Present
	Individual identification and authorization	Present
	Key management	Present
	Token and certificate standards	Present
Enclave computing environment	Access for need-to-know	Present
	Audit record content	Present
	Audit trail, monitoring, analysis, and reporting	Present
	Changes to data	Present
	Data change controls	Present
	Interconnection among systems and resources	Present
	Audit of security label changes	Present
	logon	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	Present
	Warning message	Present
	Boundary mechanism	Present
	Remote access for privileged functions	Present
Business continuity	Protection of backup and restoration of assets	Present
	Data backup procedures	Present
	Disaster and recovery planning	Present
	Backup copies of critical software	Present
	Trusted recovery	Absent
Vulnerability and incident management	Vulnerability management	Present

E) Application security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name	status
Application data handling	Database management system	Present
	Data storage	Present
	In-memory data handling	Present
	Data transmission	Present
	Data integrity	Present
	Data marking	Absent
Authentication	Server authentication	Present
	User authentication	Present
	Signed code Identification	Present
	Standalone application authentication	Present
	Server application authentication	Present
	Client application authentication	Present
	Client-server application authentication	Present
	Application component authentication	Present
	PKI certificate validation	Present
	Password complexity and maintenance	Present
	Authentication credentials protection	Present
Cryptography	Symmetric cryptography	Present
	Use of message authentication codes	Absent
	Use of digital signatures	Present
User accounts	Account rules	Present
	Account lockout policy	Present
	Avoiding duplicate accounts	Present
	Application sessions	Present
	Access control	Present
Input validation	User input validation	Present
	Web encoding	Present
	Race condition	Present
	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 access	Present
Testing	Test plans and procedures	Present
	Automated tools	Absent
Deployment	Documentation	Present
	auditing	Present

F) Wireless security risk management implementation controls and policies:

Cybersecurity implementation control type	Control name	status
Wireless WAN risk management	IEEE 802.11x Extensible authentication protocol	Present
	EAP-Transport layer security	Present
	EAP-Tunneling transport layer security	Absent
	Protected extensible authentication protocol	Present
	Separation of network	Present
	VPN	Present
	User authentication and data encryption services	Present
	Wi-fi protected access	Present
	Service set identifier (SSID)	Present
	Access point and client identification	Present
	RSN, WRAP, CCMP protocol	Present
Wireless PAN Risk management	Bluetooth specification	Present
	Device-level authentication	Present
	Data encryption	Present
	Pairing or bonding	Present
	Confidentiality, integrity, authentication, and authorization	Present
	Security models and levels	Present
	Secure simple pairing	Absent
	Key management	Present
Wireless WAN security	Use of cellular digital packet data (CDPD)	Absent

Wireless RFID Risk management	Radio frequency identifier tag encryption	Present
Wireless PED Risk management	Subscriber Identity module	Present
	Wireless email	Present
	PDA Security	Present

A list of critical assets:

ASSET ID	ASSET NAME	VALUE IN $
A_1	Personal identifiable information	$500000
A_2	Financial resources	$550000
A_3	Server	$350000
A_4	Database	$450000
A_5	Laptops and desktops	$550000
A_6	Trust	Intangible asset
A_7	Reputation	Intangible asset

List of the potential vulnerabilities for the critical assets where cybersecurity implementation controls were missing:

1. Unauthorized access
2. Information theft
3. Improper modification of data
4. Improper error diagnosis
5. Database attack
6. Network sniffing
7. MITM
8. Social engineering
9. Absence of encryption techniques
10. DDOS attack
11. Session hijacking
12. Loss of data
13. Wireless attack
14. Disclosure of sensitive information

List of the potential threats for the critical assets where cybersecurity implementation controls were missing:

1. Modification of data
2. Loss of sensitivity to information
3. Loss of ID Card and badges
4. Loss of information
5. Loss of data integrity

6. Sniffing of traffic and information
7. Modification of data by intruders
8. Loss of CIA triad and privacy to data
9. Unauthorized access
10. Sabotage communication
11. Malware intrusion
12. MITM attack
13. DNS hijacking
14. Modification and access of data by intruders
15. Loss of data
16. Unauthorized access
17. Information theft
18. Improper modification of data
19. Improper error diagnosis
20. Database attack

List of the potential risks for the critical assets where cybersecurity implementation controls were missing:

1. Loss of integrity and unauthorized viewing of data during transfer across a network
2. Loss of data and unauthorized modification due to improper security standards. Disclosure and selling of sensitive information.
3. Tampering of biometric information to get access to resources and rooms.
4. Absence of the second authentication process due to which any intruder with credentials can log in and access the employee portal.
5. Social engineering can be used to get answers to security questions and illegally access the employee portal.
6. Loss of ID Card and badges due to theft paves way for unauthorized access to assets, resources, and rooms.
7. Unauthorized modification of scanner strip
8. Social engineering is used to get ID Card and badges.
9. Modification of data by intruders
10. Loss of sensitivity to information
11. Loss of CIA triad and privacy to data
12. Loss of information
13. Unauthorized access
14. Degradation of system immunity to resist attacks
15. Malware intrusion
16. Allowing untrusted or malicious traffic

17. Sabotage communication
18. MITM attack
19. DNS hijacking
20. Session hijacking
21. Trojan and malware
22. Lack of sufficient knowledge about database functionality
23. Loss of consistency and accuracy of data.
24. Malware intrusion Loss of CIA triad and privacy to data
25. Loss of consistency and accuracy of data.
26. Loss of sensitivity to data
27. Loss of availability of resources

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 (it is not required to write detailed policies) – Risk Prevention Strategy

1. To prevent unauthorized access to the application, the security measures and framework to access the database and user accounts need to be strengthened. The use of security questions as an additional authentication process is to be employed.
2. Constant monitoring of the existing security policies against the potential threats that can occur.
3. Use of anti-virus and firewalls to protect the wireless devices against viruses and any type of malware.
4. Timely updating the anti-virus software.
5. Use of Bastion host as it can host services to withstand attacks.
6. Securing the wireless connections can prevent the occurrence of a Man-In-The-Middle attack.
7. Using a strict password policy and unique username for accessing and configuring the routers
8. Acknowledging each change to the modification of configurations and functionality of the Wireless modems and routers.
9. Using proper encryption techniques to protect the wireless network devices
10. Recognizing critical assets and making a note of the vulnerabilities and working on eliminating the vulnerabilities or reducing the impact that might occur when the vulnerabilities are exploited.
11. Using a proper database schema to prevent attacks such as SQL injection.

12. Ensuring that all 7 normal forms are properly followed while designing the database.
13. Use of access points to eliminate the unintended incoming packets to the network.

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 (it is not required to write detailed policies) – Risk Response Strategy

1. Risk cannot be eliminated completely but proper response strategies can be applied to eliminate the impact caused.
2. Periodically auditing the database functionality and transactions.
3. Timely update of software and also anti-virus software to match the current security requirements.
4. Ensuring that all the employees are aware of the security strategies and standards of the security level of the firm.
5. Having an update of the various security attacks and the measures being taken worldwide in various firms.
6. Preparation of a business contingency plan to ensure that various operations of the firm are unaffected and are functioning as normal.
7. Continuous monitoring of the audit logs and immediate reporting of unusual activity to the management.
8. Having a backup of the data and securely storing it.
9. Getting the backup a trusted approval.
10. Properly configuring the IDS, IPS, Firewall, and router to allow only trusted traffic.
11. Designing the network infrastructure to ensure that the risk that has impacted one node or resources doesn’t affect the working of the other nodes or resources.
12. The validity and authenticity of the certificates that are used to run the firm applications should be checked.
13. Alienating the task of dealing with risk management scenarios by transferring the risk to a third party who is responsible to deal with risk management and impact.
14. Ensuring that the risk plans prepared are effective in reducing risks and are functioning as intended.

For InnoFirm:

1. Ensure that data is encrypted while in storage and transmission

2. The ports can be protected by configuring to ensure that traffic is accepted from approved MAC addresses only.
3. Installing and updating the firewall to ensure that malicious traffic is filtered and ensuring the use of a hybrid firewall to have the proxy to lessen the burden on the firewall.
4. Reducing the interdependency between the network devices to ensure that it doesn't affect the functionality of the enterprise when one of the network devices is compromised.
5. Ensuring that defense-in-depth methodology is used to filter tunneled IP packets to restrict malicious traffic.
6. Ensuring that the backup reserves and data centres are present at different locations.
7. Regularly auditing and monitoring the audit logs to detect any unintended and unexpected events.
8. Monitoring that all the security controls are in place and are being followed properly.
9. Enforcing Denial of service to stop the execution of service when the system has been compromised.
10. Having a trusted backup of the data.
11. Preparing a business continuity plan to ensure that the continuity of business operations hasn't been affected after an attack has occurred.

Applicable government and regulations industry standard:

1. **Federal Managers' Financial Integrity Act:** The Federal Managers' Financial Integrity Act (FMFIA) mandates that agencies implement internal control and financial systems that offer reasonable confidence of meeting three internal control objectives:

   a) Operational effectiveness and efficiency.
   b) Observance of all applicable regulations and legislation and
   c) Financial reporting's trustworthiness.

   The agency head is required by FMFIA to deliver an annual Statement of Assurance on whether or not the agency has completed these standards. Circular A-123, Management's Responsibility for Internal Control, issued by the Office of Management and Budget (OMB), administers the FMFIA and outlines management's responsibility for internal control in federal agencies. Internal control over programs, financial reporting, and financial management systems is required by the FMFIA.

2. **Sarbanes Oxeley Act:** The Sarbanes–Oxley Act of 2002 is a federal law enacted in the United States that requires firms to follow particular financial record-keeping and

reporting procedures. The act, also known as the "Public Company Accounting Reform and Investor Protection Act" (in the Senate) and the "Corporate and Auditing Accountability, Responsibility, and Transparency Act" (in the House), and more commonly known as Sarbanes–Oxley, Sarbox, or SOX, contains eleven sections that place requirements on all US public company boards of directors and management, as well as public accounting firms. A number of provisions of the Act, such as the wilful destruction of evidence to obstruct a federal investigation, also apply to privately held businesses. The rule was passed in response to many major corporate and accounting scandals, including those involving Enron and WorldCom. The bill's parts address the board of directors' obligations, increase criminal penalties for some types of wrongdoing, and require the Securities and Exchange Commission to issue regulations defining how public firms must comply with the legislation.

3. **Gramm Leech Bliley act:** Financial institutions, or companies that give consumers financial products or services such as loans, financial or investment advice, or insurance, are required by the Gramm-Leach-Bliley Act to explain their information-sharing policies to their clients and to preserve sensitive data. Commercial banks, investment banks, securities firms, and insurance businesses were all allowed to merge after the Gramm–Leach–Bliley Act was passed. It also failed to provide the Securities and Exchange Commission (SEC) or any other financial regulatory agency the authority to regulate huge investment bank holding firms. President Bill Clinton signed the Act into law.

4. **Federal Managers' Financial Integrity Act of 1982:** The Federal Managers' Financial Integrity Act of 1982 modifies the Accounting and Auditing Act of 1950 to require federal agencies to adopt internal accounting and administrative controls to: (1) avoid waste or misappropriation of agency funds or property; and (2) ensure asset accountability. Establishes procedures for reviewing such controls by the Director of the Office of Management and Budget, in collaboration with the Comptroller General. Directs the director of each agency to examine such controls on an annual basis and submit to Congress and the President either a statement that the controls are adequate or a report on any shortcomings in the controls, together with a plan for corrective action. Requires that such declarations and reports be made public, with the exception of any classified materials.

5. **General data protection regulation Act (GDPR):** The General Data Protection Regulation (GDPR) is a regulatory framework that establishes standards for the acquisition and processing of personal data from European Union citizens (EU). Because the Regulation applies to all websites that attract European visitors, even if they do not specifically promote products or services to EU residents, it must be followed by all sites that attract European visitors. According to the GDPR, EU visitors must be provided with a number of data disclosures. In addition, the site must take efforts to assist EU consumer rights such as timely notification in the event of a data

breach. The Regulation, which was adopted in April 2016, went into full effect in May 2018 after a two-year transition period.

Rank asset risks, vulnerability risks for your company across Access control, network infrastructure, network infrastructure management, database, application, and wireless:

Domain	Top 5 asset risks	Top 5 asset vulnerabilities
Access control	Loss of confidentiality of data	Information theft
	unauthorized viewing of data	Loss of data integrity and confidentiality
	unauthorized modification	Sensitive information disclosure
	Unauthorized modification of scanner strip	Insecure storage
	MAC spoofing	Network-based attack
Network infrastructure	Improper detection of malicious traffic on the network.	Improper security controls and tools
	Stealing and accessing sensitive information	Unsecure wireless network
	Session Hijacking if the unused sessions are not closed properly	Improper session management
	There is a loss of data packets during transmission or improper packet delivery. This can also lead to unauthorized access to the nodes due to spoofing of IP addresses	IP address spoofing
	Malware intrusion to the packets during delivery	Network based attack
Network infrastructure management	Rerouting of packets due to change in router table configuration	Distributed denial of service
	Malware intrusion to the packets during delivery	Trojans and worms
	unauthorized access to the nodes due to spoofing of IP addresses	IP address spoofing
	Session Hijacking if the unused sessions are not closed properly	Improper session management

	Stealing and accessing sensitive information	Unsecure wireless network
Database	Unauthorized or faulty modifications to the database records.	Unauthorized access
	Unauthorized access to the database records due to improper authentication or access control list.	Sensitive information disclosure
	Any intruder can gain access to the accounts of the firm by simply brute-forcing with well-known credentials.	Obvious passwords for accounts
	Intruder access to data and resources due to open unused sessions	Session hijacking
	Unintended access and loss of privacy to data	DDOS
Application	It can lead to a loss of consistency and accuracy of data	Improper data marking
	The absence of screening the messages for authenticity can lead to unauthorized access and malware intrusion	Absence of MAC
	If audit trails are not secured properly, they can be modified by unauthorized personnel, they can be stolen, and also the information containing	Unauthorized access
	This can result in delay or improper diagnosis of errors and test case results.	Manual error diagnosis
	Inconsistencies in the working of application.	Malware intrusion
Wireless	Network sniffing by intruders to modify data and functionality of assets.	Improper network configuration
	Unauthorized access to resources and data.	Improper key management
	Unintended access to wireless network	Unauthorized access
	Sniffing data across wireless network while transmission	Unencrypted data

	Loss of confidentiality to resources	Firewall bypass

Top 5 potential vulnerabilities:

1. Information theft
2. Unsecure wireless network
3. Unauthorized access
4. Unencrypted data
5. Insecure storage

Top 5 potential risks:

1. Loss of CIA of data
2. Incorrect error diagnosis
3. Loss of data consistency and accuracy
4. Loss of sensitivity to data
5. Inconsistencies in various functionalities

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 (it is not required to write detailed policies) – Risk Prevention Strategy

1. To prevent unauthorized access to the application, the security measures and framework to access the database and user accounts need to be strengthened. The use of security questions as an additional authentication process is to be employed.
2. Using properly configured software and tools to detect any unintended functionalities in the network, applications, and database schema.
3. Using a strict password policy and unique username for the accounts to prevent unintended access.
4. Properly securing the wireless connections can prevent the occurrence of a Man-In-The-Middle attack and transmission of encrypted data
5. Monitoring the working of anti-virus and updating it to the latest versions upon release.
6. Recognizing critical assets and making a note of the vulnerabilities and working on eliminating the vulnerabilities or reducing the impact that might occur when the vulnerabilities are exploited.
7. Use of access points to eliminate the unintended incoming packets to the network.

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 (it is not required to write detailed policies) – Risk Response Strategy

1. Periodically auditing the database functionality and transactions. And monitoring the audit logs when a breach has occurred.
2. Restoration of data from a trusted backup.
3. Ensuring the presence of a well-designed business continuity plan.
4. Separating the compromised assets or resources.
5. Restoration of the resources to normal state after treating them accordingly.
6. Enforcing Denial of service to stop the execution of service when the system has been compromised.

Cybersecurity workforce risk management implementation

List of cybersecurity speciality areas that exist at InnoFirm

1. Risk management (RSK)
2. Software development (DEV)
3. System architecture
4. Technology R & D
5. System requirements Planning
6. Test and evaluation (TST)
7. Systems development (SYS)
8. Data administration (DTA)
9. Knowledge management (KMG)
10. Customer service and technical support (STS)
11. Network services (NET)
12. System administration (ADM)
13. System analysis (ANA)
14. Training, education and, awareness (TEA)
15. Cybersecurity management (MGT)
16. Executive cyber leadership (EXL)
17. Program/project management (PM) and acquisition
18. Cybersecurity defence analysis

19. Cyber defense infrastructure support

20. Incident response (CIR)

21. Vulnerability assessment and management (VAM)

22. Threat analysis

23. Exploitation analysis

24. All source analysis

25. Targets

26. Language analysis

27. Collection operations (CLO)

28. Cyber operational planning

29. Cyber operations (OPS)

30. Cyber investigation

31. Digital forensics

List of cybersecurity work roles that exist at InnoFirm:

1. Authorizing official/designating representative

2. security control assessor

3. software developer

4. secure software assessor

5. System test and evaluation specialist

6. System developer

7. Information systems security developer

8. Database administrator

9. Technical support specialist

10. Network operations specialist

11. Information Systems security manager

12. IT investment/Portfolio manager

13. IT program auditor

14. Cyber defense incident reporter

15. Vulnerability assessment analyst

List of cybersecurity tasks that exist at InnoFirm

TASKS
T0145: Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
T0221:Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
T0371: Establish acceptable limits for the software application, network, or system.
T0495: Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
T0184: Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.
T0244: Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
T0251: Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).
T0371: Establish acceptable limits for the software application, network, or system.
T0177: Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.
T0178: Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.
T0181: Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
T0205: 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).
T0243: Verify and update security documentation reflecting the application/system security design features.
T0264: Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.
T0268: Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.

T0309: Assess the effectiveness of security controls.
T0344: Assess all the configuration management (change configuration/release management) processes.
T0009: Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.
T0011: Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.
T0013: Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.
T0034: Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.
T0046: Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.
T0077: Develop secure code and error handling.
T0171: Perform integrated quality assurance testing for security functionality and resiliency attack.
T0189: 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.
T0311: Consult with customers about software system design and maintenance.
T0455: Develop software system testing and validation procedures, programming, and documentation.
T0553: Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.
T0028: Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
T0037: Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
T0424: Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.
T0436: Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.
T0457: Develop system testing and validation procedures, programming, and documentation.

T0516: Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.
T0554: Determine and document software patches or the extent of releases that would leave software vulnerable.
T0521: Plan implementation strategy to ensure that enterprise components can be integrated and aligned.
T0542: Translate proposed capabilities into technical requirements.
T0555: 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.
T0557: Integrate key management functions as related to cyberspace.
T0050: Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.
T0051: 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.
T0071: 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).
T0203: Provide input on security requirements to be included in statements of work and other appropriate procurement documents.
T0268: Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.
T0328: 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.
T0427: Analyze user needs and requirements to plan architecture.
T0250: Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.
T0327: Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.
T0329: Follow software and systems engineering life cycle standards and processes.
T0409: Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.

T0547: Research and evaluate available technologies and standards to meet customer requirements.
T0033: Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.
T0039: Consult with customers to evaluate functional requirements.
T0127: Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.
T0191: Prepare use cases to justify the need for specific information technology (IT) solutions.
T0300: Develop and document User Experience (UX) requirements including information architecture and user interface requirements.
T0313: Design and document quality standards.
T0454: Define baseline security requirements in accordance with applicable guidelines.
T0497: Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.
T0125: Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
T0257: Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.
T0426: Analyze the results of software, hardware, or interoperability testing.
T0513: Perform operational testing.
T0539: Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.
T0540: Record and manage test data.
T0012: Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.
T0015: Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
T0021: Build, test, and modify product prototypes using working models or theoretical models.
T0055: Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.

T0056: 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.
T0070: Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.
T0107: 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).
T0119: 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.
T0201: Provide guidelines for implementing developed systems to customers or installation teams.
T0228: Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
T0008: Analyze and plan for anticipated changes in data capacity requirements.
T0139: Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.
T0210: Provide recommendations on new database technologies and architectures.
T0306: Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.
T0422: Implement data management standards, requirements, and specifications.
T0459: Implement data mining and data warehousing applications.
T0490: Install and configure database management systems and software.
T0007: Analyze and define data requirements and specifications.
T0068: Develop data standards, policies, and procedures.
T0342: Analyze data sources to provide actionable recommendations.
T0351: Conduct hypothesis testing using statistical processes.
T0366: Develop strategic insights from large data sets.
T0381: Present technical information to technical and nontechnical audiences.

T0383: Program custom algorithms.
T0392: Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.
T0403: 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).
T0460: Develop and implement data mining and data warehousing programs.
T0037: Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.
T0060: Develop an understanding of the needs and requirements of information end-users.
T0185: Plan and manage the delivery of knowledge management projects.
T0421: Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).
T0452: Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization’s intellectual capital.
T0524: Promote knowledge sharing between information owners/users through an organization’s operational processes and systems.
T0237: Troubleshoot system hardware and software.
T0308: Analyze incident data for emerging trends.
T0315: Develop and deliver technical training to educate others or meet customer needs.
T0482: Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.
T0491: Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.
T0494: Administer accounts, network rights, and access to systems and equipment.
T0530: Develop a trend analysis and impact report.
T0035: Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).

T0081: Diagnose network connectivity problem.
T0129: Integrate new systems into existing network architecture.
T0232: Test and maintain network infrastructure including software and hardware devices.
T0029: Conduct functional and connectivity testing to ensure continuing operability.
T0136: Maintain baseline system security according to organizational policies.
T0418: Install, update, and troubleshoot systems/servers.
T0458: Comply with organization systems administration standard operating procedures.
T0498: Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.
T0514: Diagnose faulty system/server hardware.
T0515: Perform repairs on faulty system/server hardware.
T0015: Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.
T0016: Apply security policies to meet security objectives of the system.
T0086: Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.
T0169: Perform cybersecurity testing of developed applications and/or systems.
T0194: Properly document all systems security implementation, operations, and maintenance activities and update as necessary.
T0309: Assess the effectiveness of security controls.
T0006: Advocate organization's official position in legal and legislative proceedings.
T0102: Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.
T0465: Develop guidelines for implementation.
T0478: Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.
T0230: Support the design and execution of exercise scenarios.

T0248: Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.
T0345: Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.
T0380: Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.
T0442: Create training courses tailored to the audience and physical environment.
T0451: Participate in development of training curriculum and course content.
T0536: Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).
T0030: Conduct interactive training exercises to create an effective learning environment.
T0247: Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.
T0352:Conduct learning needs assessments and identify requirements.
T0395: Write and publish after action reviews.
T0025: Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.
T0044: Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.
T0095: Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.
T0229: Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
T0001: Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.
T0074: Develop policy, programs, and guidelines for implementation.
T0116: Identify organizational policy stakeholders.
T0226: Serve on agency and interagency policy boards.

T0094: Establish and maintain communication channels with stakeholders.
T0425: Analyze organizational cyber policy.
T0441: Define and integrate current and future mission environments.
T0472: Draft, staff, and publish cyber policy.
T0529: Provide policy guidance to cyber management, staff, and users.
T0002: Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.
T0006: Advocate organization's official position in legal and legislative proceedings.
T0148: Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.
T0229: Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.
T0254: Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.
T0927: Appoint and guide a team of IT security experts.
T0066: Develop and maintain strategic plans.
T0199: Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.
T0256: Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
T0196: Provide advice on project costs, design concepts, or design changes.
T0277: Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.
T0354: Coordinate and manage the overall service provided to a customer end-to-end.
T0377: Gather feedback on customer satisfaction and internal service performance to foster continual improvement.
T0207: Provide ongoing optimization and problem-solving support.

T0256: Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.
T0302: Develop contract language to ensure supply chain, system, network, and operational security are met.
T0220: Resolve conflicts in laws, regulations, policies, standards, or procedures.
T0493: Lead and oversee budget, staffing, and contracting.
T0223: Review or conduct audits of information technology (IT) programs and projects.
T0412: Conduct import/export reviews for acquiring systems and software.
T0415: Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.
T0020: Develop content for cyber defense tools.
T0043: Coordinate with enterprise-wide cyber defense staff to validate network alerts.
T0166: Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.
T0187: Plan and recommend modifications or adjustments based on exercise results or system environment.
T0258: Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.
T0042: Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.
T0335: Build, install, configure, and test dedicated cyber defense hardware.
T0438: Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).
T0486: Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.
T0047: Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.

T0163: Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.
T0170: Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.
T0214: Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.
T0010: Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.
T0252: Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).
T0550: Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).
T0569: Task Answer requests for information.
T0583: Provide subject matter expertise to the development of a common operational picture.
T0589: Assist in the identification of intelligence collection shortfalls.
T0707: Generate requests for information.
T0266: Perform penetration testing as required for new or updated applications.
T0608: Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.
T0695: Examine intercept-related metadata and content with an understanding of targeting significance.
T0775: Produce network reconstructions.
T0586: Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.
T0617: Conduct nodal analysis.
T0660: Develop information requirements necessary for answering priority information requests.
T0661: Develop measures of effectiveness and measures of performance.
T0678: Engage customers to understand customers’ intelligence needs and wants.

T0685: Evaluate threat decision-making processes.
T0686: Identify threat vulnerabilities.
T0561: Accurately characterize targets.
T0650: Determine what technologies are used by a given target.
T0717: Identify critical target elements.
T0582: Provide expertise to course of action development.
T0606: Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.
T0706: Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)
T0745: Make recommendations to guide collection in support of customer requirements.
T0837: Advise managers and operators on language and cultural issues that impact organization objectives.
T0841: Conduct all-source target research to include the use of open source materials in the target language.
T0854: Tip critical or time-sensitive information to appropriate customers.
T0573: Assess and apply operational environment factors and risks to collection management process.
T0578: Assess performance of collection assets against prescribed specifications.
T0625: Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.
T0631: Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.
T0596: Close requests for information once satisfied.
T0605: Compile lessons learned from collection management activity's execution of organization collection objectives.
T0613: Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.

T0668: Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.
T0675: Conduct and document an assessment of the collection results using established procedures.
T0682: Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.
T0714: Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.
T0576: Assess all-source intelligence and recommend targets to support cyber operation objectives.
T0590: Enable synchronization of intelligence support plans across partner organizations as required.
T0627: Contribute to crisis action planning for cyber operations.
T0680: Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.
T0703: Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.
T0733: Interpret environment preparations assessments to determine a course of action.
T0734: Issue requests for information.
TO629: 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.
T0666: Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives.
T0699: Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.
T0700: Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community.
T0759: Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.
T0598: Collaborate with development organizations to create and deploy the tools needed to achieve objectives.
T0620: Conduct open source data collection via various online tools.
T0623: Conduct survey of computer and digital networks.

T0643: Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).
T0664: Develop new techniques for gaining and keeping access to target systems.
T0677: Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.
T0059: Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.
T0096: Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).
T0110: Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.
T0120: Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.
T0419: Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.
T0403: 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).
T0425: Analyze organizational cyber policy.
T0036: Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.
T0048: Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.
T0103: Examine recovered data for information of relevance to the issue at hand.
T0165: Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.
T0173:Perform timeline analysis.

Comparison of the NCWF recommended cybersecurity speciality areas with InnoFirm’s existing cybersecurity speciality areas:

1. Risk management (RSK)	- Present
2. Software development (DEV)	- Present

3. System architecture	- Present
4. Technology R & D	- Present
5. System requirements Planning	- Present
6. Test and evaluation (TST)	- Present
7. Systems development (SYS)	- Present
8. Data administration (DTA)	- Present
9. Knowledge management (KMG)	- Present
10. Customer service and technical support (STS)	- Present
11. Network services (NET)	- Present
12. System administration (ADM)	- Present
13. System analysis (ANA)	- Present
14. Legal advice and advocacy	- Absent
15. Training, education and, awareness (TEA)	- Present
16. Cybersecurity management (MGT)	- Present
17. Strategic planning and policy (SPP)	- Absent
18. Executive cyber leadership (EXL)	- Present
19. Program/project management (PM) and acquisition	- Present
20. Cybersecurity defence analysis	- Present
21. Cyber defense infrastructure support	- Present
22. Incident response (CIR)	- Present
23. Vulnerability assessment and management (VAM)	- Present
24. Threat analysis	- Present
25. Exploitation analysis	- Present
26. All source analysis	- Present
27. Targets	- Present
28. Language analysis	- Present

WORK ROLE	TASKS	STATUS
Authorizing official	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.	Absent
	Establish acceptable limits for the software application, network, or system.	Present
	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
	Verify and update security documentation reflecting the application/system security design features.	Present
	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	Present

	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.	Present
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Present
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Assess the effectiveness of security controls.	Present
	Assess all the configuration management (change configuration/release management) processes.	Present

29. Collection operations (CLO)	- Present
30. Cyber operational planning	- Present
31. Cyber operations (OPS)	- Present
32. Cyber investigation	- Present
33. Digital forensics	- Present

Comparison of the NCWF recommended Cybersecurity work roles with InnoFirm's existing cybersecurity work roles and Comparison of the NCWF recommended Cybersecurity tasks with InnoFirm's existing cybersecurity tasks :

WORK ROLE	TASKS	STATUS
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.	Absent
	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Present
	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	absent
	Verify and update security documentation reflecting the application/system security design features.	Present
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Present

WORK ROLE	**TASKS**	**STATUS**
Software developer	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	Present
	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	Present
	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Present
	Apply secure code documentation.	Present
	Capture security controls used during the requirements phase to integrate security within the process,	Present

	to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	
	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	Present
	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	Present
	Consult with engineering staff to evaluate interface between hardware and software.	Present
	Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.	Present
	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	Present
	Develop secure code and error handling.	Absent
	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Present
	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

WORK ROLE	**TASKS**	**STATUS**
Secure software assessor	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code	Present

	scanning tools, and conduct code reviews.	
	Apply secure code documentation.	Present
	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Present
	Perform integrated quality assurance testing for security functionality and resiliency attack.	Absent
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	absent
	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	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.	Present
	Perform penetration testing as required for new or updated applications.	Present
	Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.	Present
	Determine and document software patches or the extent of releases that would leave software vulnerable.	Present

WORK ROLE	**TASKS**	**STATUS**
Enterprise architect	Define appropriate levels of system availability based on	Present

	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.	Absent
	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Absent
	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Absent
	Provide advice on project costs, design concepts, or design changes.	Present
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Present
	Analyze candidate architectures, allocate security services, and select security mechanisms.	Present
	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	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.	Present
	Analyze user needs and requirements to plan architecture.	Present

WORK ROLE	**TASK**	**STATUS**
Security architect	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Present
	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Present
	Provide advice on project costs, design concepts, or design changes.	Present
	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	Present
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle	Present

	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.	Absent
	Analyze candidate architectures, allocate security services, and select security mechanisms.	Absent
	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Present
	Assess and design security management functions as related to cyberspace.	Present

Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle suppo
Build, test, and modify product prototypes using working models or theoretical models.
Design and develop cybersecurity or cybersecurity-enabled products.
Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.
Develop and direct system testing and validation procedures and documentation.
Develop architectures or system components consistent with technical specifications.
Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing pr to systems entering a production environment.
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).
Identify and prioritize essential system functions or sub-systems required to support essential capabilities or busines functions for restoration or recovery after a system failure or during a system recovery event based on overall syster requirements for continuity and availability.
Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensur that recommended products are in compliance with organization's evaluation and validation requirements.
Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
Provide guidelines for implementing developed systems to customers or installation teams.

Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cy support plans, concept of operations, operational procedures, and maintenance training materials).
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
Utilize models and simulations to analyze or predict system performance under different operating conditions.
Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) ir development environment.
Employ configuration management processes.
Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open sou products for use within a system and ensure recommended products are in compliance with organization's evaluatic and validation requirements.
Design and develop system administration and management functionality for privileged access users.
Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.
Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out cycle).
Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.
Design hardware, operating systems, and software applications to adequately address requirements.
Design to security requirements to ensure requirements are met for all systems and/or applications.
Develop detailed design documentation for component and interface specifications to support system design and development.
Develop mitigation strategies to address cost, schedule, performance, and security risks.
Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.
Implement designs for new or existing system(s).
Perform security reviews and identify security gaps in architecture.
Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials
Provide support to test and evaluation activities.
Trace system requirements to design components and perform gap analysis.
Verify stability, interoperability, portability, and/or scalability of system architecture.
Analyze user needs and requirements to plan and conduct system development.
Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.
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).

WORK ROLE	**TASK**	**STATUS**
Research and development Specialist	Review and validate data mining and data warehousing programs, processes, and requirements.	Present
	Research current technology to understand	Present

	capabilities of required system or network.	
	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.	Absent
	Collaborate with stakeholders to identify and/or develop appropriate solutions technology.	Present

WORK ROLE	**TASK**	**STATUS**
System requirements planner	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.	Present
	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).	Present

WORK ROLE	**TASK**	**STATUS**
System test and evaluation specialist	Determine level of assurance of developed capabilities based on test results.	Present
	Analyze the results of software, hardware, or interoperability testing.	Present

	Perform developmental testing on systems under development.	Present
	Perform interoperability testing on systems exchanging electronic information with other systems.	Present
	Perform operational testing.	Present
	Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.	Present
	Record and manage test data.	Present

WORK ROLE	**TASK**	**STATUS**
Information systems security developer	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Present
	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Present
	Assess the effectiveness of cybersecurity measures utilized by system(s).	Absent
	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	Absent
	Build, test, and modify product prototypes using working models or theoretical models.	Absent
	Develop detailed security design documentation for component and interface specifications to support system design and development.	Present

	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).	Present
	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).	Present
	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.	Present
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Present
	Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements,	Present

	multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	

WORK ROLE	TASK	STATUS
Systems developer	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Present
	Build, test, and modify product prototypes using working models or theoretical models.	Present
	Design and develop cybersecurity or cybersecurity-enabled products.	Present
	Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Present
	Develop and direct system testing and validation procedures and documentation.	Present
	Develop architectures or system components consistent with technical specifications.	Present
	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Present
	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).	Present
	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

	Design hardware, operating systems, and software applications to adequately address requirements.	Present
	Provide support to test and evaluation activities.	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).	Present

WORK ROLE	TASK	STATUS
Database administrator	Analyze and plan for anticipated changes in data capacity requirements.	Present
	Maintain database management systems software.	Present
	Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.	Present
	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.	Present
	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Present
	Monitor and maintain databases to ensure optimal performance.	Present
	Perform backup and recovery of databases to ensure data integrity.	Present
	Provide recommendations on new database technologies and architectures.	Present
	Performs configuration management, problem management, capacity management, and financial	Absent

	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.	Absent
	Analyze and plan for anticipated changes in data capacity requirements.	Absent
	Develop data standards, policies, and procedures.	Present
	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Absent
	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.	Present
	Provide recommendations on new database technologies and architectures.	Absent
	Analyze data sources to provide actionable recommendations.	Present
	Assess the validity of source data and subsequent findings.	Present
	Collect metrics and trending data.	Absent
	Conduct hypothesis testing using statistical processes.	Present
	Confer with systems analysts, engineers, programmers, and others to design application.	Absent
	Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).	Present
	Develop and implement data mining and data warehousing programs.	Present

WORK ROLE	**TASK**	**STATUS**
Data analyst	Analyze and define data requirements and specifications.	Present

	Analyze and plan for anticipated changes in data capacity requirements.	Present
	Develop data standards, policies, and procedures.	Present
	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Absent
	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.	Absent
	Develop strategic insights from large data sets.	Present
	Develop and implement data mining and data warehousing programs.	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.	Absent

WORK ROLE	**TASK**	**STATUS**
Knowledge manager	Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.	Absent
	Develop an understanding of the needs and requirements of information end-users.	Present
	Monitor and report the usage of knowledge management assets and resources.	Present
	Plan and manage the delivery of knowledge management projects.	Present
	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	Present

	management and information sharing.	
	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.	Present
	Promote knowledge sharing between information owners/users through an organization's operational processes and systems.	Present

WORK ROLE	**TASK**	**STATUS**
Technical support analyst	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Present
	Troubleshoot system hardware and software.	Present
	Analyze incident data for emerging trends.	Present
	Develop and deliver technical training to educate others or meet customer needs.	Present
	Maintain incident tracking and solution database.	Absent
	Diagnose and resolve customer reported system incidents, problems, and events.	Absent
	Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.	Present
	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	Present
	Administer accounts, network rights, and access to systems and equipment.	Present
	Perform asset management/inventory of	Present

	information technology (IT) resources.	
	Monitor and report client-level computer system performance.	Present
	Develop a trend analysis and impact report.	Present

WORK ROLE	**TASK**	**STATUS**
Network operations specialist	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).	Present
	Develop and implement network backup and recovery procedures.	Absent
	Diagnose network connectivity problem.	Present
	Implement new system design procedures, test procedures, and quality standards.	Present
	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Present
	Install or replace network hubs, routers, and switches.	Absent
	Integrate new systems into existing network architecture.	Present
	Monitor network capacity and performance.	Present
	Patch network vulnerabilities to ensure that information is safeguarded against outside parties.	Absent
	Provide feedback on network requirements, including network architecture and infrastructure.	Present
	Test and maintain network infrastructure including software and hardware devices.	Present

WORK ROLE	**TASK**	**STATUS**
System administrator	Conduct functional and connectivity testing to ensure continuing operability.	Present
	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	Present

	Develop and document systems administration standard operating procedures.	Present
	Maintain baseline system security according to organizational policies.	Present
	Manage accounts, network rights, and access to systems and equipment.	Present
	Plan, execute, and verify data redundancy and system recovery procedures.	Present
	Provide ongoing optimization and problem-solving support.	Present
	Install, update, and troubleshoot systems/servers.	Absent
	Check system hardware availability, functionality, integrity, and efficiency.	Absent

WORK ROLE	**TASK**	**STATUS**
Systems security analyst	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Present
	Apply security policies to meet security objectives of the system.	Present
	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	absent
	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Present
	Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.	Present
	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Present

	Implement specific cybersecurity countermeasures for systems and/or applications.	Present
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Present
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Present

WORK ROLE	TASK	STATUS
Customer service and technical support	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Present
	Troubleshoot system hardware and software.	Present
	Analyze incident data for emerging trends.	Present
	Develop and deliver technical training to educate others or meet customer needs.	Present
	Maintain incident tracking and solution database.	Absent
	Diagnose and resolve customer reported system incidents, problems, and events.	Present
	Perform asset management/inventory of information technology (IT) resources.	Present
	Monitor and report client-level computer system performance.	Absent
	Develop a trend analysis and impact report.	Absent

WORK ROLE	TASKS	STATUS
Network services	Configure and optimize network hubs, routers, and	Present

	switches (e.g., higher-level protocols, tunneling).	
	Develop and implement network backup and recovery procedures.	Present
	Diagnose network connectivity problem.	Present
	Implement new system design procedures, test procedures, and quality standards.	Present
	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Absent
	Install or replace network hubs, routers, and switches.	Absent
	Integrate new systems into existing network architecture.	Present
	Monitor network capacity and performance.	Present
	Patch network vulnerabilities to ensure that information is safeguarded against outside parties.	Present
	Provide feedback on network requirements, including network architecture and infrastructure.	Present
	Test and maintain network infrastructure including software and hardware devices.	Absent

	Tasks	
Systems administration	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	Present
	Monitor and maintain system/server configuration.	Present
	Oversee installation, implementation, configuration, and support of system components.	Present
	Diagnose faulty system/server hardware.	Present
	Perform repairs on faulty system/server hardware.	Absent

	Troubleshoot hardware/software interface and interoperability problems.	Present

WORK ROLE	TASKS	STATUS
Systems security analyst	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Present
	Apply security policies to meet security objectives of the system.	Present
	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	Present
	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Present
	Assess the effectiveness of security controls.	Present
	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Absent
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Present
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Present

WORK ROLE	TASKS	STATUS
Privacy officer/privacy compliance manager	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Present
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security	Present

	programs, policies, processes, systems, and elements.	
	Conduct functional and connectivity testing to ensure continuing operability.	Present
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	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.	Present
	Liaise with regulatory and accrediting bodies.	Present
	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	Present
	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

WORK ROLE	**TASK**	**STATUS**
Cyber instructional curriculum developer	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Present

	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Present
	Research current technology to understand capabilities of required system or network.	Present
	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.	Present
	Conduct learning needs assessments and identify requirements.	Present
	Create interactive learning exercises to create an effective learning environment.	Present
	Develop or assist in the development of training policies and protocols for cyber training.	Present
	Develop the goals and objectives for cyber curriculum.	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.	Present

WORK ROLE	**TASKS**	**STATUS**
Cyber instructor	Conduct interactive training exercises to create an effective learning environment.	Present
	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	absent
	Evaluate the effectiveness and comprehensiveness of existing training programs.	absent
	Review training documentation (e.g., Course	Absent

	Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).	
	Support the design and execution of exercise scenarios.	Present
	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Present
	Develop or assist in the development of computer based training modules or classes.	Present
	Develop or assist in the development of course assignments.	Present
	Develop or assist in the development of course evaluations.	Present
	Develop or assist in the development of grading and proficiency standards.	Present
	Deliver training courses tailored to the audience and physical/virtual environments.	Present
	Apply concepts, procedures, software, equipment, and/or technology applications to students.	Present
	Design training curriculum and course content based on requirements.	Present
	Participate in development of training curriculum and course content.	Present
	Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.	Present
	Recommend revisions to curriculum and course content based on feedback from previous training sessions.	Present
	Serve as an internal consultant and advisor in own area of expertise (e.g., technical,	Present

	copyright, print media, electronic media).	
	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

WORK ROLE	**TASKS**	**STATUS**
Information systems security manager	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Present
	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Present
	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Absent
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Present
	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	Present
	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.	Present
	Establish overall enterprise information security	Absent

	architecture (EISA) with the organization’s overall security strategy.	
	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.	Present
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Present
	Identify alternative information security strategies to address organizational security objective.	Present
	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Present
	Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.	Present
	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	Present
	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Present
	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
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Present

	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.	Present
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Present
	Continuously validate the organization against policies/guidelines/procedures/ regulations/laws to ensure compliance.	Present
	Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.	Present
	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Present

WORK ROLE	**TASK**	**STATUS**
Communications security manager	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Present
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Present
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Present
	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Present
	Ensure that security improvement actions are evaluated, validated, and implemented as required.	Absent

	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Present
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Present
	Recognize a possible security violation and take appropriate action to report the incident, as required.	Present
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Present

WORK ROLE	TASK	STATUS
Cyber workforce developer and manager	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Present
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Present
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Present
	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Present
	Develop policy, programs, and guidelines for implementation.	Present
	Establish and maintain communication channels with stakeholders.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Present

	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	Present
	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Present

WORK ROLE	TASK	STATUS
Cyber policy and strategy planner	Develop policy, programs, and guidelines for implementation.	Present
	Establish and maintain communication channels with stakeholders.	Absent
	Review existing and proposed policies with stakeholders.	Present
	Serve on agency and interagency policy boards.	Absent
	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Absent
	Define and integrate current and future mission environments.	Present
	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.	Present
	Draft, staff, and publish cyber policy.	Present
	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Present
	Seek consensus on proposed policy changes from stakeholders.	Present
	Provide policy guidance to cyber management, staff, and users.	Present
	Review, conduct, or participate in audits of cyber programs and projects.	Present

	Support the CIO in the formulation of cyber-related policies.	Present

WORK ROLE	TASK	STATUS
Executive cyber leadership	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Absent
	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Absent
	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation	Present
	Appoint and guide a team of IT security experts.	Present
	Collaborate with key stakeholders to establish a cybersecurity risk management program.	Present

WORK ROLE	TASK	STATUS
Program manager	Develop and maintain strategic plans.	Present
	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Present
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Present
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Present
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Present
	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all	Present

	significant activities so the service is delivered successfully.	
	Coordinate and manage the overall service provided to a customer end-to-end.	Present

WORK ROLE	TASK	STATUS
Information technology program manager	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Present
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Present
	Provide advice on project costs, design concepts, or design changes.	Present
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Present
	Provide ongoing optimization and problem-solving support.	Present
	Provide recommendations for possible improvements and upgrades.	Present
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	absent
	Draft and publish supply chain security and risk management documents.	Present

WORK ROLE	TASK	STATUS
Product support manager	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Present
	Perform needs analysis to determine opportunities for new	Present

	and improved business process solutions.	
	Provide advice on project costs, design concepts, or design changes.	Present
	Provide input to implementation plans and standard operating procedures.	Present
	Provide ongoing optimization and problem-solving support.	Present
	Provide recommendations for possible improvements and upgrades.	Present
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Present
	Review or conduct audits of information technology (IT) programs and projects.	Present
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Present
	Develop and document supply chain risks for critical system elements, as appropriate.	Present
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Present
	Lead and oversee budget, staffing, and contracting.	Present
	Provide enterprise cybersecurity and supply chain risk management guidance.	Present
	Draft and publish supply chain security and risk management documents.	Present
	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Present

WORK ROLE	TASK	STATUS

IT investment/portfolio manager	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Present
	Review or conduct audits of information technology (IT) programs and projects.	Present
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Develop contract language to ensure supply chain, system, network, and operational security are met.	Present
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Present
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Present
	Lead and oversee budget, staffing, and contracting.	Present
	Draft and publish supply chain security and risk management documents.	Present

WORK ROLE	**TASK**	**STATUS**
IT program auditor	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Present
	Provide ongoing optimization and problem-solving support.	Present
	Provide recommendations for possible improvements and upgrades.	Present
	Review or conduct audits of information technology (IT) programs and projects.	Present
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Present

	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Present
	Conduct import/export reviews for acquiring systems and software.	Present
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent

WORK ROLE	**TASK**	**STATUS**
Cyber defense analyst	Develop content for cyber defense tools.	present
	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Absent
	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	present
	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Absent
	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	Present
	Perform cyber defense trend analysis and reporting.	Present
	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and	Present

	determine the effectiveness of an observed attack.	
	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Present
	Plan and recommend modifications or adjustments based on exercise results or system environment.	Present
	Provide daily summary reports of network events and activity relevant to cyber defense practices.	Present
	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Present
	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.	Present
	Reconstruct a malicious attack or activity based off network traffic.	Present
	Identify network mapping and operating system (OS) fingerprinting activities.	Present
	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.	present
	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.	Present

	Analyze and report organizational security posture trends.	Present
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Present
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Present

WORK ROLE	**TASK**	**STATUS**
Cyber defense infrastruce support specialist	Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.	present
	Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).	absent
	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).	absent
	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.	absent

WORK ROLE	**TASK**	**STATUS**
Cyber defence incident responder	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.	Present

	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.	Present
	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.	Present
	Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Present
	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Present
	Coordinate with intelligence analysts to correlate threat assessment data.	Present

WORK ROLE	**TASK**	**STATUS**
Vulnerability assessment analyst	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	Present
	Conduct and/or support authorized penetration testing on enterprise network assets.	Present
	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.	Present
	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	Present
	Prepare audit reports that identify technical and	Present

	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).	Present
	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

WORK ROLE	**TASK**	**STATUS**
Warning analyst	Answer requests for information.	Present
	Provide subject matter expertise to the development of a common operational picture.	Absent
	Maintain a common intelligence picture.	Absent
	Provide subject matter expertise to the development of cyber operations specific indicators.	Present
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Present
	Assist in the identification of intelligence collection shortfalls.	Present

	Brief threat and/or target current situations.	Present
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Present
	Conduct in-depth research and analysis.	Present
	Conduct nodal analysis.	Present
	Develop information requirements necessary for answering priority information requests.	Present
	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	present
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Present
	Report intelligence-derived significant network events and intrusions.	Present
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Present

WORK ROLE	**TASK**	**STATUS**
Exploitation analyst	Conduct and/or support authorized penetration testing on enterprise network assets.	Present
	Perform penetration testing as required for new or updated applications.	Absent
	Apply and utilize authorized cyber capabilities to enable access to targeted networks.	Present
	Apply cyber collection, environment preparation and engagement expertise to enable new exploitation	Present

	and/or continued collection operations, or in support of customer requirements.	
	Apply and obey applicable statutes, laws, regulations and policies.	Absent
	Perform analysis for target infrastructure exploitation activities.	Present
	Collaborate with other internal and external partner organizations on target access and operational issues.	Present
	Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.	Present
	Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.	Present
	Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.	Present
	Monitor target networks to provide indications and warning of target communications changes or processing failures.	Present
	Produce network reconstructions.	Present
	Profile network or system administrators and their activities.	Absent

WORKROLE	**TASKS**	**STATUS**
All source analyst	Answer requests for information.	Present
	Provide expertise to course of action development.	Present
	Provide subject matter expertise to the development of a common operational picture.	Present

	Maintain a common intelligence picture.	present
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Present
	Identify and submit intelligence requirements for the purposes of designating priority information requirements.	Present
	Identify intelligence gaps and shortfalls.	Present
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	absent
	Monitor and report on validated threat activities.	Present
	Monitor open source websites for hostile content directed towards organizational or partner interests.	Present
	Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements.	Absent
	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Provide subject matter expertise to website characterizations.	Absent
	Provide analyses and support for effectiveness assessment.	Absent
	Provide timely notice of imminent or hostile intentions or activities which may impact	Present

	organization objectives, resources, or capabilities.	
	Report intelligence-derived significant network events and intrusions.	Present

WORKROLE	**TASKS**	**STATUS**
Mission assessment specialist	Provide expertise to course of action development.	Present
	Provide subject matter expertise to the development of a common operational picture.	Present
	Provide subject matter expertise to the development of cyber operations specific indicators.	Present
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Present
	Provide expertise to the development of measures of effectiveness and measures of performance.	Present
	Conduct end-of-operations assessments.	Present
	Conduct in-depth research and analysis.	Present
	Conduct nodal analysis.	Present
	Develop munitions effectiveness assessment or operational assessment materials.	Present

WORK ROLE	**TASK**	**STATUS**
Target developer	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Present
	Conduct nodal analysis.	Present
	Conduct target research and analysis.	Present
	Coordinate target vetting with appropriate partners.	Present

	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	Present
	Determine what technologies are used by a given target.	Present
	Develop all-source intelligence targeting materials.	Absent
	Develop measures of effectiveness and measures of performance.	Present
	Develop munitions effectiveness assessment or operational assessment materials.	Present

WORK ROLE	**TASK**	**STATUS**
Target network analyst	Provide expertise to course of action development.	Present
	Classify documents in accordance with classification guidelines.	Present
	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Present
	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 nodal analysis.	Present
	Conduct quality control to determine validity and relevance of information gathered about networks.	Present
	Conduct target research and analysis.	Present
	Determine what technologies are used by a given target.	Present

WORK ROLE	**TASK**	**STATUS**

Multi-discipline language analyst	Identify collection gaps and potential collection strategies against targets.	Present
	Make recommendations to guide collection in support of customer requirements.	Present
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Present
	Advise managers and operators on language and cultural issues that impact organization objectives.	Present
	Analyze and process information using language and/or cultural expertise.	Present
	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.	Present

WORK ROLE	TASK	STATUS
All source collection manager	Assess and apply operational environment factors and risks to collection management process.	Present
	Assess performance of collection assets against prescribed specifications.	Present
	Compare allocated and available assets to collection demand as expressed through requirements.	Present
	Compile lessons learned from collection management activity's execution of organization collection objectives.	Present
	Consider efficiency and effectiveness of collection assets and resources if/when	Present

	applied against priority information requirements.	
	Construct collection plans and matrixes using established guidance and procedures.	Present

WORK ROLE	**TASK**	**STATUS**
All source collection requirements manager	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	Present
	Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.	Present
	Disseminate reports to inform decision makers on collection issues.	Present
	Conduct and document an assessment of the collection results using established procedures.	Present
	Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.	Present
	Evaluate extent to which collected information and/or produced intelligence satisfy information requests.	Present
	Evaluate extent to which collection operations are synchronized with operational requirements.	Present

WORK ROLE	**TASK**	**STATUS**
Cyber operational planning	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.	Present
	Coordinate for intelligence support to operational planning activities.	Present

	Assess all-source intelligence and recommend targets to support cyber operation objectives.	Present
	Assess target vulnerabilities and/or operational capabilities to determine course of action.	Present
	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Present
	Assist in the development and refinement of priority information requirements.	Present
	Enable synchronization of intelligence support plans across partner organizations as required.	Present

WORK ROLE	TASK	STATUS
Cyber Ops manager	Evaluate intelligence estimates to support the planning cycle.	Present
	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Present
	Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.	Present
	Incorporate cyber operations and communications security support plans into organization objectives.	Present
	Identify cyber intelligence gaps and shortfalls for cyber operational planning.	Present
	Integrate cyber planning/targeting efforts with other organizations.	Present

WORK ROLE	TASK	STATUS
Partner integration planner	Develop, maintain, and assess cyber cooperation security agreements with external partners.	Present

	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.	Present
	Identify and manage security cooperation priorities with external partners.	Present
	Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.	Present
	Integrate cyber planning/targeting efforts with other organizations.	Present
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Present
	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Present
	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	absent
	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Present
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	absent

WORK ROLE	**TASK**	**STATUS**
Cyber operator	Conduct access enabling of wireless computer and digital networks.	Present
	Conduct collection and processing of wireless	Present

	computer and digital networks.	
	Conduct exploitation of wireless computer and digital networks.	Absent
	Conduct network scouting and vulnerability analyses of systems within a network.	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.	Present
	Conduct open source data collection via various online tools.	Present
	Conduct survey of computer and digital networks.	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.	Present

WORK ROLE	**TASK**	**STATUS**
Cyber crime investigator	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.	Present
	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.	Present
	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).	Present

	Examine recovered data for information of relevance to the issue at hand.	absent
	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.	Present
	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.	Present
	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.	Present
	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Present
	Identify elements of proof of the crime.	Present

WORK ROLE	**TASK**	**STATUS**
Forensics analyst	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).	Present
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Present
	Analyze incident data for emerging trends.	Present
	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Present
	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards,	Present

	procedures, or other issuances.	
	Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.	Present

WORK ROLE	TASK	STATUS
Cyber defense forensics analyst	Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.	Present
	Decrypt seized data using technical means.	Present
	Provide technical summary of findings in accordance with established reporting procedures.	Present
	Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	Present
	Examine recovered data for information of relevance to the issue at hand.	absent
	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Present

	Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.	Present
	Perform file signature analysis.	Present
	Perform hash comparison against established database.	Present
	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).	Present
	Perform timeline analysis.	Present
	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	absent
	Perform static media analysis.	absent
	Perform tier 1, 2, and 3 malware analysis.	Present
	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	Present
	Provide technical assistance on digital evidence matters to appropriate personnel.	Present
	Recognize and accurately report forensic artifacts indicative of a particular operating system.	absent

	Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).	Present

List of potential threats to InnoFirm that could exploit vulnerabilities of critical assets due to missing cybersecurity speciality areas, cybersecurity workroles, and cybersecrutiy tasks:

1. Loss of CIA triad of resources

2. Inconsistencies in working of the resources

3. Loss of privacy to data

4. Loss of sensitivity to data

5. Unauthorized access to resources

6. Improper training and lack of security awareness

7. Improper IR and disaster management

8. Unauthorized modification of data

9. Damage to resources and data

10. Absence of business continuity plan

List of potential risks to InnoFirm that could exploit vulnerabilities of critical assets due to missing cybersecurity speciality areas, cybersecurity workroles, and cybersecrutiy tasks:

1. Loss of integrity and unauthorized viewing of data during transfer across a network

2. Loss of data and unauthorized modification due to improper security standards. Disclosure and selling of sensitive information.

3. Tampering of biometric information to get access to resources and rooms.

4. Absence of the second authentication process due to which any intruder with credentials can log in and access the employee portal.

5. Social engineering can be used to get answers to security questions and illegally access the employee portal.

6. Loss of ID Card and badges due to theft paves way for unauthorized access to assets, resources, and rooms.

7. Network spoofing due to unencrypted data and unsecure network.

8. Lack of security controls and policies to secure infrastructure and resources.

9. Unavailability of resources due to improper business contingency plan.

List of recommended policies (Hiring new cybersecurity staff, education current staff, outsourcing), for each recommended cybersecurity speciality area, workrole or task that should be created to mitigate the identified risk:

1. Constantly monitoring the audit logs to detect malicious events.

2. Enforcing stringent authentication and authorization policies by proper access control list.

3. Enforcing proper security controls and policies and ensuring that all the employees are aware of it.

4. Properly explain the roles, access to resources and procedure to safeguard the resources to all the employees.

5. Identity the critical assets of the organization.

6. Maintaing a trusted backup of the resources from a trusted senior management.

7. Documenting the security policies and controls and forward it throughout the organization.

8. Upon making a new project agreement with another company, the security controls should be viewed and assessed by the management team and they should align with the firm’s policies and controls.

9. Verification of the services of the third party to detect the presence of any unintended event before incorporating with the firms’ services.

PART –C
SECURITY RISK MANAEGMENT RECOMMENDATIONS

Provide a list of the recommendation prevention and response controls, methods and policies and their implementation costs and benefits based on your risk management analysis:

For HGA:

1. The audit logs were to monitored regularly
2. Faster installation of anti-virus, firewalls and upgrading them to the latest version.
3. Using digital signatures to verify the authenticity of the certificate and communication being transferred
4. Using a secure VPN to connect to remote desktops.
5. Lack of encryption of ports and protocols can lead to sniffing by intruders.
6. Multiple factor authentication to strengthen to authentication of the user.
7. Manual errors might lead to payroll errors hence proper analysis of the payroll data has to be done.
8. The sensitive information must be stored and transmitted securely and the recommended way it to encrypt the data.
9. Immediately reporting any unintended access or modification of data to the security team.
10. Ensuring the security controls are working accordingly and verifying if any new controls are needed to enhance the security framework.

For InnoFirm:

1. Identifying the critical assets and resources and ensuring that they are secured with the appropriate security controls and policies.

2. Using hybrid technology firewalls to have the implementation of firewall and proxy to detect incoming malicious traffic.

3. Configuring and updating the anti-virus and firewall.

4. Defining proper access privileges and access control list.

5. Periodic assessments to review the security knowledge of the employees.

6. Periodic monitoring the functionality of various resources in accordance with the security controls and policies.

7. Proper authentication and authorization techniques to grant the access to resources accordingly.

8. Alienating the task of dealing with risk management scenarios by transferring the risk to a third party who is responsible to deal with risk management and impact.

9. Ensuring that the risk plans prepared are effective in reducing risks and are functioning as intended.

For HGA:

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

= 840500 – 48984 = 791516

The budget exceeds the value of risk

Proposed security risk budget Cost:

1) Cost-benefit ratio analysis for risk prevention budget

   = Proposed risk security budget cost / expected security risk benefit

   = 549000 / 48984

   = 11.20

2) Cost-benefit ratio analysis for risk response budget

   = Proposed risk security budget cost / expected security risk benefit

   = 554000 / 48984

   = 11.30

3) Cost-benefit ratio analysis for mixed budget

   = Proposed risk security budget cost / expected security risk benefit

   = 1107000 / 48984

   = 22.59

For InnoFirm:

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

= 90000 – 55000 = 35000

The budget exceeds the value of risk

Proposed security risk budget Cost:

1) Cost-benefit ratio analysis for risk prevention budget

   = Proposed risk security budget cost / expected security risk benefit

= 650000 / 55900

= 11.62

2) Cost-benefit ratio analysis for risk response budget

= Proposed risk security budget cost / expected security risk benefit

= 578900 / 51237

= 11.29

3) Cost-benefit ratio analysis for mixed budget

= Proposed risk security budget cost / expected security risk benefit

= 1232897 / 59642

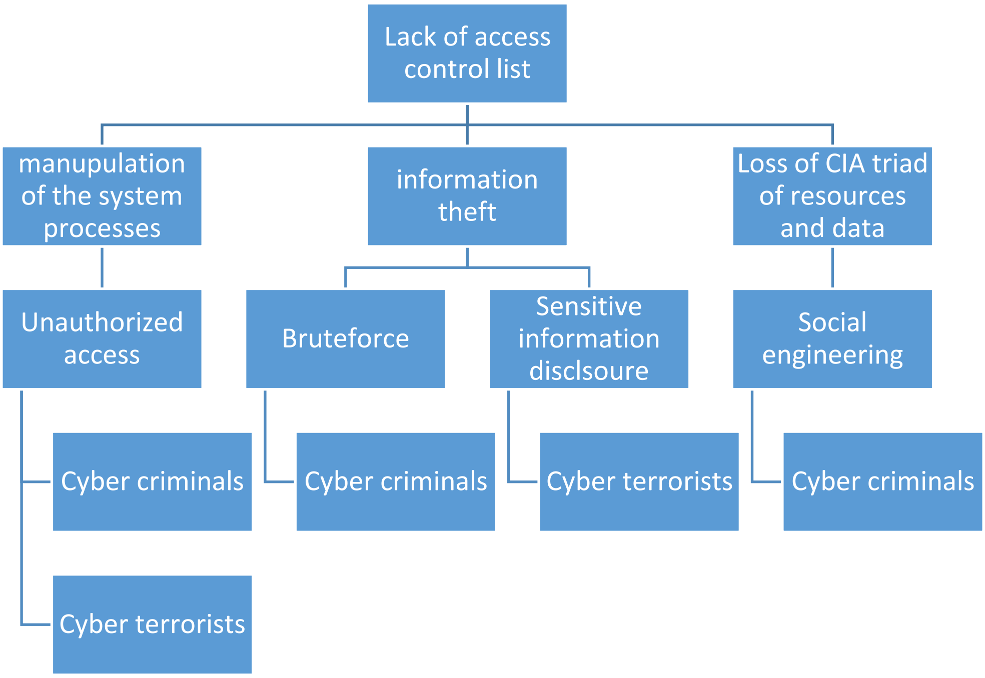
= 20.67

Comparing the proposed security controls, methods,a nd policies budget for HGA with the proposed security controls, methods and policies for InnoFirm:

Points of consideration	HGA	InnoFirm
Industry	Financial-government	Private IT firm
Mission	Transfer of finances from to various agencies and sectors of the government	InnoFirm is a cutting-edge software design and development studio that serves customers all over the world. To conceive and create the technology of the future, they collaborate with partners ranging from Fortune 500 businesses to start-ups
Geographic presence	United states of america	India
Number of employees	1000	500
Network topology	Appendix 1	Appendix 2
Critical assets $	94	
Threat environment	Hackers, other government	Competitors, insider threat
Threat agents	Cyber terrorist, cyber criminals	Black hat hackers
Residual risk	85540	90000
Budget for risk prevention and response controls, methods, policies	22.59	20.67

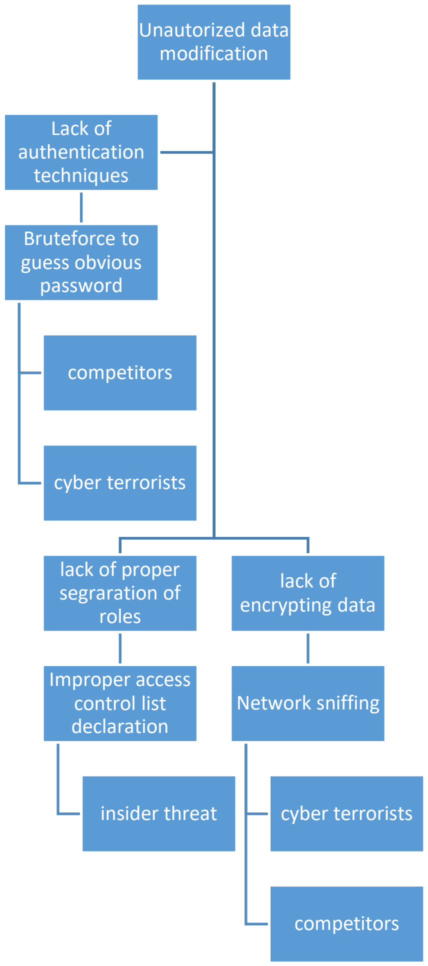
$ security budget / $ security risk improvement	0.678	0.572
$ security budget / $ critical assets	0.91	0.742
$ security budget / $ employees	495	270

ATTACK TREE FOR HGA:



The agents cyber criminals and cyber terrorists use various attacks to exploit the resources of HGA.

ATTACK TREE FOR InnoFirm:


Unautorized data modification
Lack of authentication techniques
Bruteforce to guess obvious password
competitors
cyber terrorists
lack of proper segraration of roles
lack of encrypting data
Improper access control list declaration
Network sniffing
insider threat
cyber terrorists
competitors

Vulnerabilities and exploitation probabilities:

For HGA:

Vulnerabilities	exploitation probabilities
Corrupted timesheets	48
Uauthorized access	50
Unapproved mofication of payroll data	20
Mainframe I&A system	24
Incomplete contingency planning	32
Unemployed virus prevention strategies	38
Loss of data due to no backup	17
Unsecure storage of confidential information	10
Communication of unencrypted data over a network	28

For InnoFirm:

Vulnerabilities	**exploitation probabilities**
Unauthorized access	30
Social engineering	27
Theft	38
Absence of encryption techniques	12
Unauthorized modification	16
Improper backup of resource data and state	22
Unsecure storage and transmission of data	22
Absence of proper segregation of duties	20

Cybersecurity workforce recommendation:

For HGA:

1. Proper employee security awareness and training programs should be enforced.

2. Properly training the employees and educating them about their roles and responsibilities.

3. Monitoring if all the employees are complying the security controls and policies.

4. Implementing additional controls, security soft wares when needed.

5. Having an update of the various security software used along with their configurations and versions.

For InnoFirm:

1. Use of the best encryption standards to safeguard resources and data.

2. Having a trusted backup and proper recovery strategies.

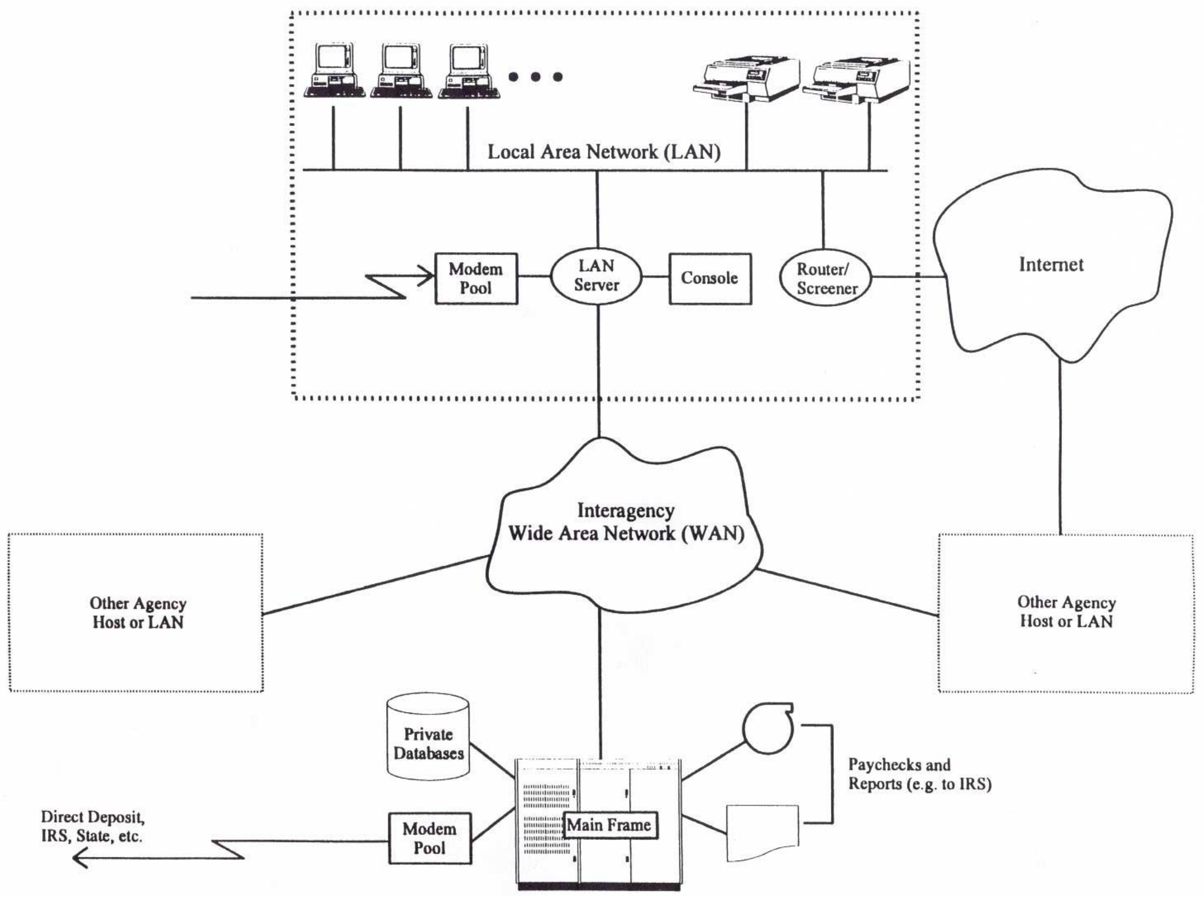
3. Proper audit techniques and monitoring the audit logs.

4. Properly segregating the roles and responsibilities of all employees and granting least privileges.

5. Immediately reporting the malicious activities to the risk management team.

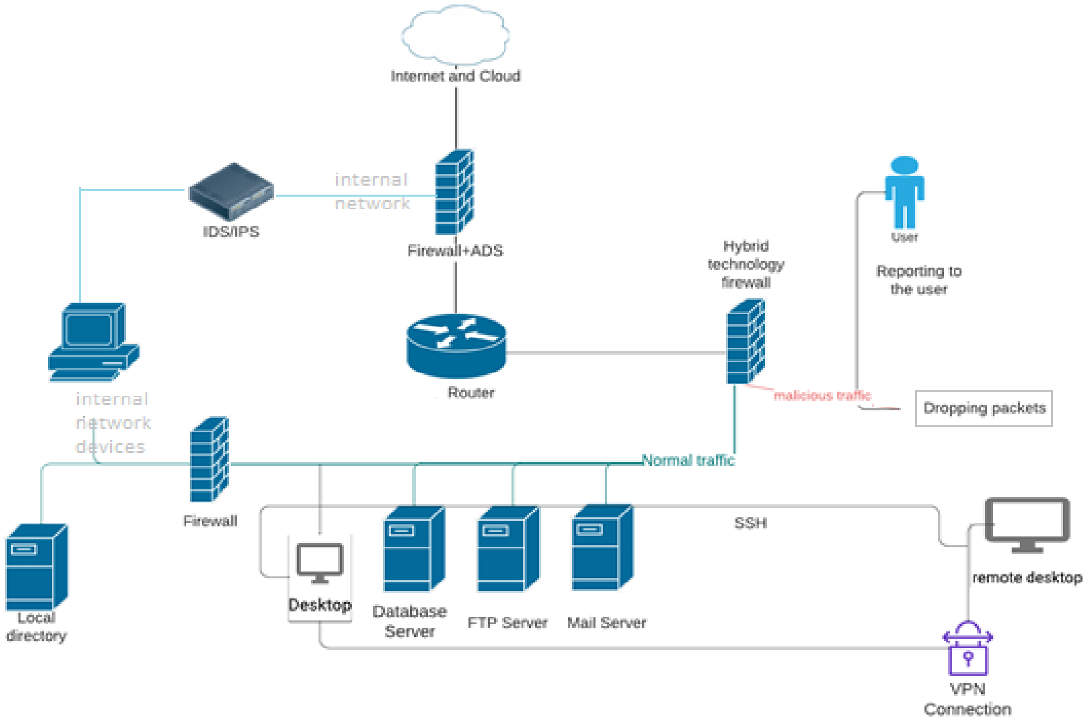
PART-D
APPENDIX

Appendix 1: Network topology diagram for HGA:



The above image describes the environment of the system with the Wide Area Network (WAN) being the network environment comprising of all the resources. It connects the Local Area Network (LAN) of HGA to the LAN of the other firms. The LAN of HGA consists of many devices that are connected to the LAN server which is the central server. The LAN server accommodates various applications across the devices of the LAN. The modem pool and router help in secure connection of the other network devices to the internet. It also consists of a special console. The WAN is connected to a mainframe, which is basically a super computer that handles various operations such as database transactions. It also consists of data related to paychecks and other reports and memos.

Appendix 2: Network topology diagram for InnoFirm:



The network diagram illustrates various network devices linked together. It consists of various firewalls which act as checkpoints to examine the incoming traffic against the security controls. Through the firewall, the traffic passes through the internal network and is examined by the IDS/IPS which further sends it to the internal network devices and database server if the traffic is not malicious. After being examined by the firewall and ADS, the router routes the traffic through the hybrid technology to the various server. The PC (desktop) can connect to the remote desktop either by SSH or by using a secure VPN connection. On detecting malicious traffic, the firewall either report it to the end-user or drops the packets. In this way, the security of the resources is monitored and maintained.

References:

- Hypothetical government agency (HGA) case study
- https://searchcompliance.techtarget.com/definition/residual-risk#:~:text=Residual%20risk%20is%20the%20risk,process%20improvements%20have%20been%20applied.
- https://www.ipohub.org/cybersecurity-laws-regulations/
- https://www.gsa.gov/reference/reports/budget-performance/annual-reports/agency-financial-report-2012/managements-discussion-and-analysis/gsa-management-assurances/federal-managers-financial-integrity-act-section-2
- https://www.law.cornell.edu/wex/sarbanes-oxley_act#:~:text=The%20Sarbanes%2DOxley%20Act%20(SOX,scandals%20in%20the%20early%2D2000s.
- https://en.wikipedia.org/wiki/Sarbanes%E2%80%93Oxley_Act
- https://en.wikipedia.org/wiki/Gramm%E2%80%93Leach%E2%80%93Bliley_Act
- https://www.ftc.gov/business-guidance/privacy-security/gramm-leach-bliley-act
- https://www.congress.gov/bill/97th-congress/house-bill/1526#:~:text=Federal%20Managers'%20Financial%20Integrity%20Act,assure%20the%20accountability%20of%20assets.
- https://www.altiusit.com/files/blog/Top10WirelessNetworkRisks.htm
- https://www.pluralsight.com/blog/it-ops/stateful-firewall-fundamentals
- https://www.bastille.net/blogs/2018/7/24/wireless-intrusion-detection-systems-wids
- https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection
- https://www.pluralsight.com/blog/it-ops/stateful-firewall-fundamentals
- https://www.bastille.net/blogs/2018/7/24/wireless-intrusion-detection-systems-wids
- https://www.fortinet.com/resources/cyberglossary/dpi-deep-packet-inspection
- https://www.stigviewer.com/stig/firewall_security_requirements_guide/2018-12-24/finding/V-79485
- https://www.transtutors.com/questions/why-is-there-a-restriction-on-the-generation-of-an-icmpv4-message-in-response-to-a-f-650784.htm
- https://www.rapid7.com/fundamentals/vulnerability-management-and-scanning/
- https://www.orbit-computer-solutions.com/vlan-trunking-protocol-vtp/
- https://www.tp-link.com/us/configuration-guides/configuration_guide_for_802_1x_vlan_assignment_and_mab/?configurationId=2968
- https://iopscience.iop.org/article/10.1088/1742-6596/1714/1/012045/pdf
- https://www.venafi.com/blog/why-are-man-middle-attacks-so-dangerous-venafi#:~:text=Attackers%20might%20use%20MitM%20attacks,Turedi%2C%20technology%20strategist%20at%20CrowdStrike.

- https://www.techrepublic.com/article/10-things-you-should-know-about-securing-dns/
- https://insights.samsung.com/2021/04/22/3-ways-you-can-mitigate-man-in-the-middle-attacks-3/
- http://www.free-management-ebooks.com/faqpm/risk-05.htm
- SANS VPN Policy: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt9071f38721fd20f3/5e9e0ae2b17045600041974d/virtual_private_network_policy.pdf
- SANS Remote access tools policy: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt0a307ae2bb5b3b62/5e9dfa093acb0660063feb59/remote_access_tools_policy.pdf
- https://blog.newtoniannuggets.com/the-mythical-application-owner-and-why-they-matter-to-devops-2a39bd6b0057#:~:tex*t=An%20application%20owner%20is%20the,application%2C%20including%20appropriate%20security%20safeguards.
- https://www.aits.uillinois.edu/access/get_access/get_data_warehouse_access/info_for_users/about_application_accounts/#:~:text=Application%20accounts%20are%20defined%20as,technical%20staff%20support%20the%20application.
- https://www.fortinet.com/resources/cyberglossary/digital-certificates
- https://www.manageengine.com/device-control/data-replication.html
- https://csrc.nist.gov/csrc/media/publications/shared/documents/itl-bulletin/itlbul1997-03.txt
- https://blog.sift.com/2015/you-can-label-me/
- https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt9cafed12ccd9856c/5e9dd6bad275f070a0330b26/web_application_security_policy.pdf
- https://www.securew2.com/solutions/802-1x#:~:text=802.1X%20is%20a%20network,confirmed%20by%20the%20RADIUS%20server.
- https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html
- https://en.wikipedia.org/wiki/Extensible_Authentication_Protocol
- https://www.cert.govt.nz/it-specialists/critical-controls/network-segmentation-and-separation/#:~:text=Separation%20means%20using%20different%20types,access%20controls%20or%20security%20policies.
- https://www.techopedia.com/definition/5049/cellular-digital-packet-data-cdpd
- https://www.simbase.com/iot-glossary-dictionary/subscriber-identity-module#:~:text=The%20SIM%20is%20an%20integrated,a%20telephone%20book%20and%20messages.
- SANS Wireless communication policy: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blte0e352dc1934ea5f/5e9dfb76d5a1cb709eee4a6e/wireless_communication_policy.pdf

- SANS Wireless communication standard: https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt836d5fac43a8727f/5e9dfd035661cd12411d53a6/wireless_communication_standard.pdf