# Security Risk Assessment and Management class paper

Namruth Reddy S
suryanarayanareddy.n@northeastern.edu

# Table of Contents

# Part A

# Executive Summary

Information System Name: Hypothetical Government Agency

Information System Categorization:

| Asset | Info Security Elements | | |
|---|---|---|---|
| | **Confidentiality** | **Integrity** | **Availability** |
| A1. Financial resources | High | High | Medium |
| A2. System components (PCs, LAN server) | Low | Low | Medium |
| A3. Personal Information | High | High | Medium |
| A4. Contracting and Procurement documents | Medium | Medium | Low |
| A5. Draft regulations | Medium | High | Medium |
| A6. Internal correspondence | Medium | High | Low |
| A7. Business documents | High | High | Medium |

Organization name: Hypothetical Government Agency

Organization address: 822 Huntington Ave, Boston, MA

Namruth Reddy

Title: Chief Executive Officer
Email: namruth@email.com
Phone: +1-857-123-4567

Prashant Mohan

Title: Chief Information Officer
Email: prashant@email.com
Phone: +1-857-123-4568

Gokul Ganne

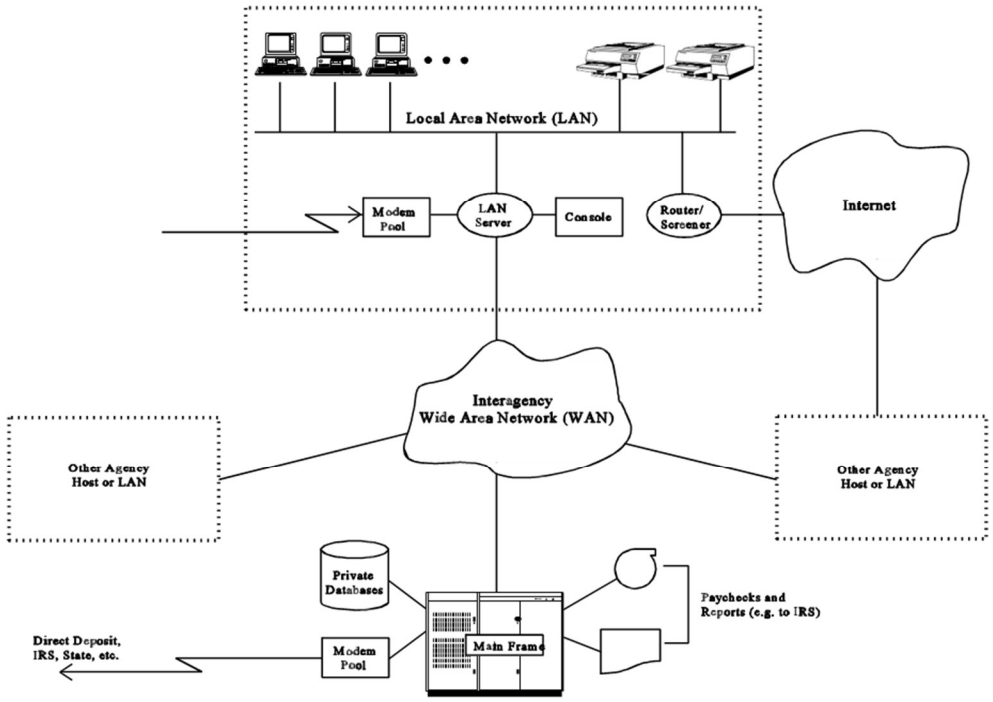
Title: Chief Financial Officer
Email: gokul@email.com
Phone: +1-857-123-4569

Darshan GM

Title: Chief Information Security Officer
Email: darshan@email.com
Phone: +1-857-123-4579
Information System Type: Major Application

System Description: Funds transfer from US government to contractors

System Environment:




The environment shows the Wide Area Network (WAN) which connects all the agencies which have their own Local Area Networks( LAN). The mainframe computer is connected to the private database and the modem pool. It also has paychecks and reports regarding the organization.

**Interconnection of System Information:**

System Name: Government Agency

Type of Organization: Public Sector Telecommunication Industry

Type of Agreement: Government Contract

Date: April 31, 1996

FIPS 199 Category: High (H)

C&A Category: Accredited and Certified

Authorizing Official: Namruth Reddy

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

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

**Minimum Security Controls:**

| Security Control | Observations | Status | Content Type | Responsible Authority |
|---|---|---|---|---|
| Information Security Audits (M1) | The Identification of information security audits is performed regularly | In Progress | Common | CIO |
| Compliance &Regulatory Audits (M2) | Compliance and regulatory audits have been identified | Complete | Common | CIO |
| Segregation of Duties (M3) | Duties are segregated to different levels to reduce risk | Complete | Common | CISO |

| | | | | |
|---|---|---|---|---|
| Standards and Policies (M4) | Applicable policies and standards. have been adhered to. | In Progress | Common | CIO |
| Security & Awareness Training (M5) | Awareness Programs are carried out to educate the staff on security. | In Progress | Common | CISO |
| Security Incident Management (M6) | SIEM is considered as an important step | Complete | Common | CISO |
| Backups (M7) | Backups are scheduled. | In Progress | Common | CISO |
| Contingency Planning (M8) | Contingency Planning is in process. | Complete | Common | CISO |
| Data Privacy Policy (M9) | Drafting of DPP is in process. | In Progress | Common | CIO |
| Event Management (M10) | SIEM Process establishment is in process | In Progress | Common | CISO |
| Resource Management (M11) | Allocation of resources is performed to the acceptable level. | Complete | Common | CISO |
| Usage of Automated Access Control Mechanisms (M13) | Automated systems are introduced to reduce manual effort | Complete | Common | CISO |
| Data Redundancy Control (M14) | Data redundancy is increased to avoid risk | Complete | Common | CISO |
| Installing Firewalls (M15) | Firewalls are installed on the servers. | Complete | Common | CISO |

Information Security Plan Complete Date: 02/18/2021
Information Security Plan Approval Date: 02/21/2021

## List of Assets

Assuming HGA has around 150 employees. These are the approximate estimated values of assets listed for the company. All values listed are in thousands.

I believe personal information has the highest value among all of these assets. System components such as PCs or routers are definitely not as valuable as the personal information or reputation of the company. Other values are approximated based on research around similar organizations and their asset values. Check for references used at the end of the assignment.

| Asset | $ value (In thousand) |
|---|---|
| A1. Financial resources | 700 |
| A2. System components (PCs, LAN server) | 500 |
| A3. Personal Information | 950 |
| A4. Contracting and Procurement documents | 800 |
| A5. Draft regulations | 400 |
| A6. Internal correspondence | 300 |
| A7. Business documents | 800 |
| A8. Reputation | 850 |
| A9. Employee confidence | 800 |
| A10. VPN Server | 250 |
| A11. DMZ | 300 |

## List of threats

| |
|---|
| T1: Payroll Fraud |
| T2: Payroll Errors |
| T3: Interruption of Operations |
| T4: Disclosure or Brokerage of information |
| T5: Network-Related Attacks |
| T6: Other threats - natural disasters or threats we cant directly control |

## List of security vulnerabilities

| Threats | Vulnerabilities |
|---|---|
| T1: Payroll Fraud | V1.1: Falsified Time Sheets<br>V1.2: Unauthorized Access<br>V1.3: Bogus Time and Attendance Applications<br>V1.4: Unauthorized Modifications of Time and Attendance Sheets |
| T2: Payroll Errors | V2: Vulnerabilities Related to Payroll Errors - late submission of personnel paperwork |
| T3: Interruption of Operations | V3.1: COG Contingency Planning - improper verification<br>V3.2: Division Contingency Planning - improper delegation to COG<br>V3.3: Virus Prevention<br>V3.4: Accidental Corruption and Loss of Data |
| T4: Disclosure or Brokerage of information | V4: Vulnerabilities Related to Disclosure or Brokerage of information - improper logins and sniffer programs |
| T5: Network-Related Attacks | V5: Vulnerabilities Related to Network-Related Attacks - email utility vulnerability and |

| | |
|---|---|
| | evaesdropping |

## Subset of Critical Assets

| Asset | $ value (in thousands) |
|---|---|
| A2. System components | $500 |
| A3. Personal Information | $950 |
| A7. Business documents | $800 |
| A8. Reputation | $850 |
| A9. VPN Server | $250 |
| A10. DMZ | $300 |

## Subset of Threats

| Threat |
|---|
| T2: Payroll Errors |
| T3: Interruption of Operations |
| T4: Disclosure or Brokerage of information |
| T5: Network-Related Attacks |
| T6: Other threats - natural disasters or threats we cant directly control |

## Subset of Vulnerabilities

| Vulnerabilities |
|---|
| V2: Vulnerabilities Related to Payroll Errors - Unauthorized access |
| V3: COG improper contingency planning |
| V4: Vulnerabilities Related to Disclosure or Brokerage of information -lack of compliance with policies and |

| |
|---|
| procedures |
| V5: Vulnerabilities Related to Network-Related Attacks - Vulnerable email utility and eavesdropping |
| V6. Attackers exploiting bad configurations in newly setup devices |

## Threat Vulnerabilities pairs on asset subset - A2,A3,A7,A8,A9,A10

| | **T2** | **T3** | **T4** | **T5** | **T6** |
|---|---|---|---|---|---|
| **V2** | 25 | 20 | 25 | 20 | 25 |
| **V3** | 25 | 25 | 20 | 15 | 20 |
| **V4** | 20 | 10 | 15 | 15 | 15 |
| **V5** | 20 | 20 | 10 | 15 | 10 |
| **V6** | 15 | 20 | 15 | 20 | 15 |

1. Vulnerabilities related to payroll errors are majorly affected by threats from payroll errors and disclosure or brokerage of information. These probability values for this vulnerability are assigned accordingly.

2. COG improper contingency planning is one of the key vulnerabilities in the HGA organization. It is extremely important to have a thorough contingency plan for any organization and probabilities of each threat are valued based on improper contingency planning

3. Vulnerabilities Related to Disclosure or Brokerage of information is mainly due to lack of compliance with policies and procedures. This can mainly lead to the disclosure of information and other threats. This vulnerability is assigned values in the table accordingly.

4. Vulnerabilities Related to Network-Related Attacks is due to vulnerable email utility and eavesdropping. This can lead to serious security attacks as systems exposed to the internet have a very high chance of getting compromised and this can lead to serious other attacks once the attacker is able to compromise one internal system.

## Asset/vulnerability pairs

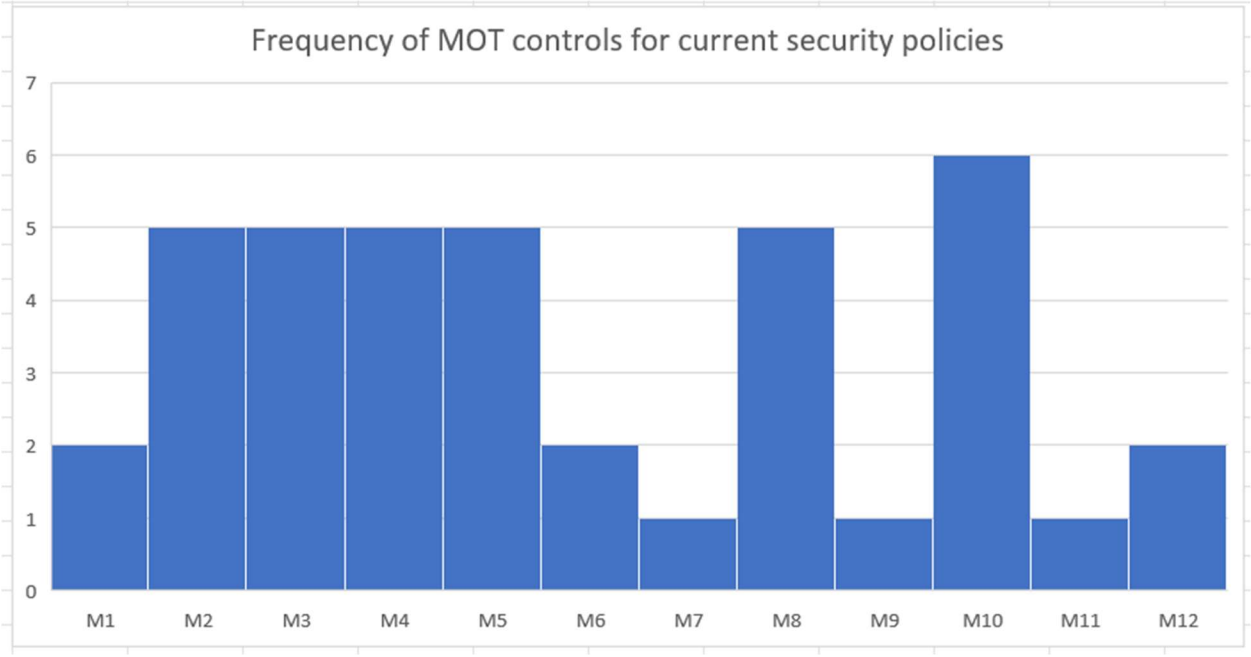
| Asset | Vulnerabilities |
|---|---|
| A2. System components | V4: Vulnerabilities Related to Disclosure or Brokerage of information.<br>V5: Vulnerabilities Related to Network-Related Attacks |
| A3. Personal Information | V4: Vulnerabilities Related to Disclosure or Brokerage of information<br>V3.4: Accidental Corruption and Loss of Data |
| A7. Business documents | V3.4: Accidental Corruption and Loss of Data<br>V4: Vulnerabilities Related to Disclosure or Brokerage of information |
| A8. Reputation | V2: Vulnerabilities Related to Payroll Errors |

Some of the management-operational-technical controls suggested in the case study are:

| Management | Operational | Technical |
|---|---|---|
| Security audits - M1 | Security awareness training - M5 | Access control - M10 |
| Compliance and regulatory audits -M2 | Security incident management - M6 | Data redundancy - M11 |
| Duties segregation - M3 | Backups - M7 | Firewalls - M12 |
| Standards and policies - M4 | Contingency planning - M8 | |
| | Hardware security - M9 | |

# Current security controls and policies mapped to MOT controls

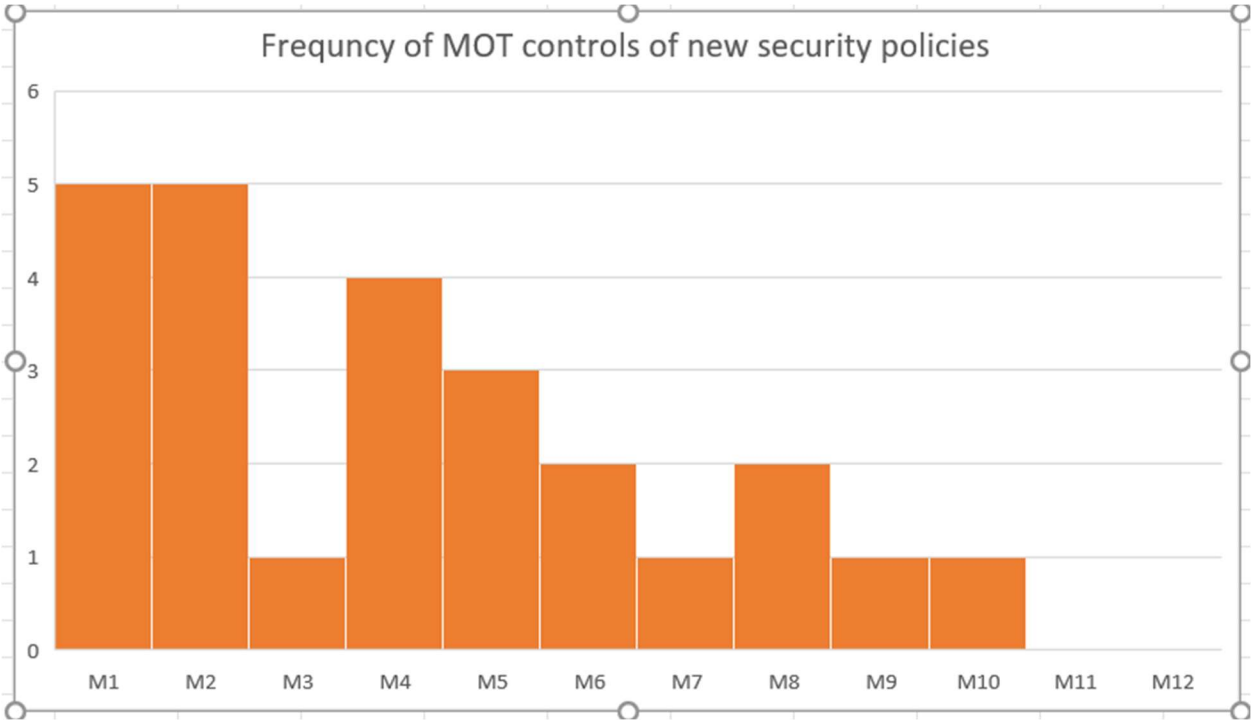
| Policy | Description | MOT control mapping |
|---|---|---|
| HGA's Computer Operations Group (COG) - | Responsible for General Use and Administration of HGA's Computer System | 3,4,5,8 |
| Time and Attendance Application - Protection Against Payroll Fraud and Errors | Protection Against Unauthorized Execution Applying access control policies by admins | 1,2,3,5,8,10 |
| | Protection Against Payroll Errors - Frequency of data entry and approvals by supervisors | 2,3,4,10 |
| | Protection Against Accidental Corruption or Loss of Payroll Data - Using backups and error checking during transmission | 3,5,8,9,10,11 |
| Protection Against Interruption of Operations | COG Contingency Planning - plan for natural disasters or equipment malfunctions | 2,4,6,8,7 |
| | Division Contingency Planning - addresses critical business functions and acceptable interruption periods | 2,4,6,8 |
| Protection Against Disclosure or Brokerage of Information | PCs need to be locked | 5,10 |
| | Access control by administrators | 3,5,10 |
| | Security awareness training | 4,5 |
| Protection Against Disclosure or Brokerage of Information | Packet filtering for outgoing traffic in routers | 12 |
| | Network access controls by administrators | 10,12 |
| Protection Against Risks from Non–HGA Computer Systems | Written permissions from the controlling organizations | 1,2,10 |




## Proposed security controls and policies mapped to MOT controls

| Policy | Description | MOT mapping |
|---|---|---|
| Controls Mitigating Vulnerabilities Related to Payroll Fraud | Server Administrative procedures and bugfixes | 2,4,10 |
| | Use of one time passwords | 1,2 |
| | Use of digital signatures | 1,2,4 |
| Controls Mitigating Payroll Error | Incentives for complying and using digital signatures | 2,5 |
| Controls Mitigating Vulnerabilities Related to Continuity of Operations | Contingency plan training | 1,4,6,8 |
| | Automated E-mail Reminders and Back-ups | 6,7 |

| | | |
|---|---|---|
| Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information | Screen locks, | 5,10,9 |
| | Hard Disk Encryption | 9,4,8 |
| Controls Vulnerabilities Related to NetworkRelated Attacks | Stronger I&A, | 1,3,5 |
| | Encrypting modems, | 1,2 |
| | Mainframe Communications Encryption | 1,4,9 |



## Scenario - Security Risk Prevention Strategy

Compare the list of current security controls and the new CISO proposed controls and policies, with the Risk Management Controls model we discussed in class, i.e. Management-Operational-Technical controls. Include any missing M-O-T controls and then apply a Security Risk Prevention
Strategy and a Security Risk Response (Resilience) Strategy by

**Security Risk Prevention Strategy Step P1**: Calculate updated Residual Risk Rankings and Vulnerability Risk Rankings due to updated threat/vulnerability pairs with further reduced probabilities due to implementing M-O-T controls which reduce threat/vulnerability probabilities. Keep risk impacts at Initial value of 100% for worst-case scenario

| | **Threat X Vulnerability - Threat exploiting a vulnerability (All values in percentage)** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Asset** | T2* V2 | T2* v3 | T2* V4 | T2* V5 | T2* V6 | T3* V2 | T3* v3 | T3* V4 | T3* V5 | T3* V6 | T4* V2 | T4* v3 | T4* V4 | T4* V5 | T4* V6 | T5* V2 | T5* v3 | T5* V4 | T5* V5 | T5* V6 |
| A2 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A3 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A7 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A8 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A9 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A10 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |

| | **Threat X Vulnerability - Threat exploiting a vulnerability (All values in percentage)** | | | | |
|---|---|---|---|---|---|
| **Asset** | T6*V2 | T6*v3 | T6*V4 | T6*V5 | T6*V6 |
| A2 | 100 | 100 | 100 | 100 | 100 |
| A3 | 100 | 100 | 100 | 100 | 100 |

| | | | | | |
|---|---|---|---|---|---|
| A7 | 100 | 100 | 100 | 100 | 100 |
| A8 | 100 | 100 | 100 | 100 | 100 |
| A9 | 100 | 100 | 100 | 100 | 100 |
| A10 | 100 | 100 | 100 | 100 | 100 |

## Threat Vulnerabilities pairs on asset subset - A2,A3,A7,A8,A9,A10

| | **T2** | **T3** | **T4** | **T5** | **T6** |
|---|---|---|---|---|---|
| **V2** | 25 | 20 | 25 | 20 | 25 |
| **V3** | 25 | 25 | 20 | 15 | 20 |
| **V4** | 20 | 10 | 15 | 15 | 15 |
| **V5** | 20 | 20 | 10 | 15 | 10 |
| **V6** | 15 | 20 | 15 | 20 | 15 |

Risk of V2 = 115
Risk of V3 = 105
Risk of V4 = 75
Risk of V5 = 75
Risk of V6 = 85
Total threat = 455

| **Asset** | **$ value (in thousands)** | **Total threat** | **Residual risk** |
|---|---|---|---|
| **A2** | 500 | 455 | 2275000 |
| **A3** | 950 | 455 | 4322500 |
| **A7** | 800 | 455 | 3640000 |
| **A8** | 850 | 455 | 3867500 |
| **A9** | 250 | 455 | 1137500 |
| **A10** | 300 | 455 | 1365000 |

**Calculate residual vulnerability security risks**

Risk due to V2 = [(500*115)+(950*115)+(800*115)+(850*115)+(250*115)+(300*115)]/100 = 4197500
Risk due to V3 = [(500*105)+(950*105)+(800*105)+(850*105)+(250*105)+(300*105)]/100 = 3832500
Risk due to V4 = [(500*75)+(950*75)+(800*75)+(850*75)+(250*75)+(300*75)]/100 = 2737500
Risk due to V5 = [(500*75)+(950*75)+(800*75)+(850*75)+(250*75)+(300*75)]/100 = 2737500
Risk due to V6 = [(500*85)+(950*85)+(800*85)+(850*85)+(250*85)+(300*85)]/100 = 3102500

**Ranking of security asset residual risk**

| Asset | Residual risk | Rank |
|---|---|---|
| **A3** | 4322500 | 1 |
| **A8** | 3867500 | 2 |
| **A7** | 3640000 | 3 |
| **A2** | 1830000 | 4 |
| **A10** | 1365000 | 5 |
| **A9** | 1137500 | 6 |

**Ranking of vulnerability security risks**

| Vulnerability | Vulnerability security risk | Rank |
|---|---|---|
| **V2** | **4197500** | **1** |
| **V3** | 3832500 | 2 |
| **V6** | 3102500 | 3 |
| **V4** | 2737500 | 4 |
| **V5** | 2737500 | 5 |

## Security risk prevention strategy P2

HGA management decided to replace the modem pool with a VPN server and add a screened subnet with DMZ. Apply these Hardening Controls to highest ranked Vulnerability Risk, with updated reduced probabilities, thus 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 in $ from the M-O-T Controls in Step P1 (!).

## Threat Vulnerabilities pairs on asset subset - A2,A3,A7,A8, A9,A10

| | T2 | T3 | T4 | T5 | T6 |
|---|---|---|---|---|---|
| **V2** | 5 | 7 | 6 | 5 | 5 |
| **V3** | 25 | 25 | 20 | 15 | 20 |
| **V4** | 20 | 10 | 15 | 15 | 15 |
| **V5** | 20 | 20 | 10 | 15 | 10 |
| **V6** | 15 | 20 | 15 | 20 | 15 |

Risk of V2 = 28
Risk of V3 = 105
Risk of V4 = 75
Risk of V5 = 75
Risk of V6 = 85
Total threat = 366

| Asset | $ value (in thousands) | Total threat | Residual risk |
|---|---|---|---|
| **A2** | 500 | 366 | 1830000 |
| **A3** | 950 | 366 | 3477000 |
| **A7** | 800 | 366 | 2928000 |
| **A8** | 850 | 366 | 3111000 |
| **A9** | 250 | 366 | 915000 |
| **A10** | 300 | 366 | 1098000 |

**Residual vulnerability security risks**

Risk due to V2 = [(500*28)+(950*28)+(800*28)+(850*28)+(250*28)+(300*28)]/100 = 1022000
Risk due to V3 = [(500*105)+(950*105)+(800*105)+(850*105)+(250*105)+(300*105)]/100 = 3832500
Risk due to V4 = [(500*75)+(950*75)+(800*75)+(850*75)+(250*75)+(300*75)]/100 = 2737500

Risk due to V5 = [(500*75)+(950*75)+(800*75)+(850*75)+(250*75)+(300*75)]/100 = 2737500
Risk due to V6 = [(500*85)+(950*85)+(800*85)+(850*85)+(250*85)+(300*85)]/100 = 3102500

**Ranking of security asset residual risk**

| Asset | Residual risk | Rank |
|---|---|---|
| **A3** | 3477000 | 1 |
| **A8** | 3111000 | 2 |
| **A7** | 2928000 | 3 |
| **A2** | 1830000 | 4 |
| **A10** | 1098000 | 5 |
| **A9** | 915000 | 6 |

**Ranking of vulnerability security risks**

| Vulnerability | Vulnerability security risk | Rank |
|---|---|---|
| **V3** | **3832500** | **1** |
| **V6** | 3102500 | 2 |
| **V4** | 2737500 | 3 |
| **V5** | 2737500 | 4 |
| **V2** | 1022000 | 5 |

## Security risk prevention strategy P3

Apply additional Hardening Controls to new now highest ranked Vulnerability Risk, thus further reducing the security asset residual risks 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 Hardening Controls in Step P2 (!)

After applying better access control rules and reducing the risk and re-calculating the overall risk, we see that V3.1: COG improper contingency planning has the highest risk now.

COG improper contingency planning can be reduced by asking users to store the backup in LAN server than PCs so that even if PCs go down, backups are still intact. Administrators are advised to only use licensed copyrighted software so that viruses can be avoided.

After implementing these controls to reduce the risk of V3, these are the updated values:

## Threat Vulnerabilities pairs on asset subset - A2,A3,A7,A8,A9,A10

| | T2 | T3 | T4 | T5 | T6 |
|---|---|---|---|---|---|
| **V2** | 5 | 7 | 6 | 5 | 5 |
| **V3** | 4 | 5 | 6 | 4 | 20 |
| **V4** | 20 | 10 | 15 | 15 | 15 |
| **V5** | 20 | 20 | 10 | 15 | 10 |
| **V6** | 15 | 20 | 15 | 20 | 15 |

Risk of V2 = 28
Risk of V3 = 39
Risk of V4 = 75
Risk of V5 = 75
Risk of V6 = 85
Total threat = 300

| Asset | $ value (in thousands) | Total threat | Residual risk |
|---|---|---|---|
| **A2** | 500 | 300 | 150000 |
| **A3** | 950 | 300 | 285000 |
| **A7** | 800 | 300 | 240000 |
| **A8** | 850 | 300 | 255000 |
| **A9** | 250 | 300 | 75000 |
| **A10** | 300 | 300 | 90000 |

**Residual vulnerability security risks**

Risk due to V2 = [(500*28)+(950*28)+(800*28)+(850*28)+(250*28)+(300*28)]/100 = 1022000
Risk due to V3 = [(500*39)+(950*39)+(800*39)+(850*39)+(250*39)+(300*39)]/100 = 1423500
Risk due to V4 = [(500*75)+(950*75)+(800*75)+(850*75)+(250*75)+(300*75)]/100 = 2737500
Risk due to V5 = [(500*75)+(950*75)+(800*75)+(850*75)+(250*75)+(300*75)]/100 = 2737500
Risk due to V6 = [(500*85)+(950*85)+(800*85)+(850*85)+(250*85)+(300*85)]/100 = 3102500

**Ranking of security asset residual risk**

| Asset | Residual risk | Rank |
|---|---|---|
| **A3** | 285000 | 1 |
| **A8** | 255000 | 2 |
| **A7** | 240000 | 3 |
| **A2** | 150000 | 4 |
| **A10** | 90000 | 5 |
| **A9** | 75000 | 6 |

**Ranking of vulnerability security risks**

| Vulnerability | Vulnerability security risk | Rank |
|---|---|---|
| **V6** | 3102500 | 1 |
| **V4** | 2737500 | 2 |
| **V5** | 2737500 | 3 |
| **V3** | 1423500 | 4 |
| **V2** | 1022000 | 5 |

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

All the controls listed were part of the 157 risk controls in the common criteria such as contingency planning, configuration management, incident response, awareness and training. List also included technical security controls such as access control and system and communication protection.

## Security Risk response (resilience) strategy

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

### Security risk prevention strategy R1

### Threat Vulnerabilities pairs on asset subset - A2,A3,A7,A8,A9,A10

| | **T2** | **T3** | **T4** | **T5** | **T6** |
|---|---|---|---|---|---|
| **V2** | 5 | 7 | 6 | 5 | 5 |
| **V3** | 4 | 5 | 6 | 4 | 20 |
| **V4** | 20 | 10 | 15 | 15 | 15 |
| **V5** | 20 | 20 | 10 | 15 | 10 |
| **V6** | 15 | 20 | 15 | 20 | 15 |

**Updated risk impacts**

| | **Threat X Vulnerability - Threat exploiting the vulneability** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Assets** | T2* V2 | T2* v3 | T2* V4 | T2* V5 | T2* V6 | T3* V2 | T3* v3 | T3* V4 | T3* V5 | T3* V6 | T4* V2 | T4* v3 | T4* V4 | T4* V5 | T4* V6 | T5* V2 | T5* v3 | T5* V4 | T5* V5 | T5* V6 |
| **A2** | 60 | 50 | 30 | 40 | 50 | 50 | 60 | 30 | 40 | 50 | 50 | 60 | 30 | 50 | 50 | 50 | 60 | 30 | 40 | 50 |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A3** | 30 | 40 | 50 | 30 | 50 | 60 | 30 | 30 | 30 | 50 | 40 | 40 | 50 | 30 | 50 | 60 | 40 | 40 | 30 | 50 |
| **A7** | 50 | 50 | 40 | 30 | 50 | 50 | 60 | 50 | 40 | 50 | 40 | 30 | 30 | 30 | 50 | 30 | 40 | 50 | 40 | 50 |
| **A8** | 40 | 40 | 60 | 40 | 50 | 50 | 30 | 40 | 60 | 50 | 40 | 50 | 30 | 50 | 50 | 30 | 60 | 60 | 40 | 50 |
| **A9** | 60 | 50 | 30 | 40 | 50 | 50 | 60 | 30 | 40 | 50 | 50 | 60 | 30 | 50 | 50 | 50 | 60 | 30 | 40 | 50 |
| **A10** | 30 | 40 | 50 | 30 | 50 | 60 | 30 | 30 | 30 | 50 | 40 | 40 | 50 | 30 | 50 | 60 | 40 | 40 | 30 | 50 |

| | **Threat X Vulnerability - Threat exploiting a vulnerability (All values in percentage)** | | | | |
|---|---|---|---|---|---|
| **Asset** | T6*V2 | T6*v3 | T6*V4 | T6*V5 | T6*V6 |
| A2 | 50 | 50 | 50 | 50 | 50 |
| A3 | 50 | 50 | 50 | 50 | 50 |
| A7 | 50 | 50 | 50 | 50 | 50 |
| A8 | 50 | 50 | 50 | 50 | 50 |
| A9 | 50 | 50 | 50 | 50 | 50 |
| A10 | 50 | 50 | 50 | 50 | 50 |

## Residual Asset security risks

### Risk of Assest A2:

500*(5*60+4*50+6*30+5*40 + 15*50+7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50+ 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50) /10 = 59200

### Risk of Asset A3

950*(5*30+4*40+6*50+5*30+15*50+7*60+5*30+4*30+7*30+20*50+6*40+6*40+8*50+8*30+15*50+5*60+4*40+7*40+4*30+20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 108205

### Risk of Asset A7

800*(5*50+4*50+6*40+5*30+15*50+7*50+5*60+4*50+7*40+20*50+6*40+6*30+8*30+8*30+15*50+5*30+4*40+7*40+4*40+20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 90960

**Risk of Asset A8**

850*(5*40+4*40+6*60+5*40+15*50+7*50+5*30+4*40+7*60+20*50+6*40+6*50+8*30+8*50+15*50+5*30+4*60+7*60+4*40+20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 101150

**Risk of Asset A9**

250*(5*60+4*50+6*30+5*40 + 15*50+ 7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50 + 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 29600

**Risk of Asset A10**

300*(5*60+4*50+6*30+5*40 + 15*50+ 7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50 + 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 35520

## Residual vulnerability security risks

**Risk due to V2**

(500*(5*60+7*50+6*50+5*50+5*50) + 950*(5*30+7*60+6*40+5*60+5*50) +
800*(5*50+7*50+6*40+5*30+5*50) +850*(5*40+7*50+6*40+5*30+5*50) +
250*(5*60+7*50+6*50+5*50+5*50) + 300*(5*30+7*60+6*40+5*60+5*50))/10 = 479100

**Risk due to V3**

(500*(4*50+5*60+6*60+4*60+20*50) + 950*(4*40+5*60+6*40+4*40+20*50) +
800*(4*50+5*60+6*30+4*40+20*50) +850*(4*40+5*30+6*50+4*60+20*50) +
250*(4*50+5*60+6*60+4*60+20*50) + 300*(4*40+5*60+6*40+4*40+20*50))/10 = 694450

**Risk due to V4**

(500*(6*30+4*30+8*30+7*30+15*50) + 950*(6*50+4*30+8*50+7*40+15*50) +
800*(6*40+4*50+8*30+7*50+15*50) +850*(6*60+4*40+8*30+7*60+15*50) +
250*(6*30+4*30+8*30+7*30+15*50) + 300*(6*50+4*30+8*50+7*40+15*50))/10 = 650200

**Risk due to V5**

(500*(5*40+7*40+8*50+4*40+10*50) + 950*(5*30+7*30+8*30+4*30+10*50) +
800*(5*30+7*40+8*30+4*40+10*50) +850*(5*40+7*60+8*50+4*40+10*50) +
250*(5*40+7*40+8*50+4*40+10*50) + 300*(5*30+7*30+8*30+4*30+10*50))/10 = 517200

**Risk due to V6**

(500*(15*50+20*50+15*50+20*50+15*50) + 950*(15*50+20*50+15*50+20*50+15*50) + 800*(15*50+20*50+15*50+20*50+15*50) +850*(15*50+20*50+15*50+20*50+15*50) + 250*(15*50+20*50+15*50+20*50+15*50) + 300*(15*50+20*50+15*50+20*50+15*50))/10 = 1551250

## Ranking of security asset residual risk

| Asset | Residual risk | Rank |
|---|---|---|
| **A3** | **108205** | **1** |
| **A8** | 101150 | 2 |
| **A7** | 90960 | 3 |
| **A2** | 59200 | 4 |
| **A10** | 35520 | 5 |
| **A9** | 29600 | 6 |

## Ranking of vulnerability security risks

| Vulnerability | Vulnerability security risk | Rank |
|---|---|---|
| **V6** | 1551250 | 1 |
| **V3** | 694450 | 2 |
| **V4** | 650200 | 3 |
| **V5** | 517200 | 4 |
| **V2** | 479100 | 5 |

## Security risk response strategy 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 (!).

We see that asset A3 - Personal Information has the highest residual risk according to calculations in R1. PII is one the of the biggest assets in modern day organizations. Its extremely important to keep it encrypted with the latest cryptographic algorithms so that even if hackers get past the security they still cant read it.

Update values after applying the response strategy are:

## Threat Vulnerabilities pairs on asset subset - A2,A3,A7,A8,A9,A10

| | **T2** | **T3** | **T4** | **T5** | **T6** |
|---|---|---|---|---|---|
| **V2** | 5 | 7 | 6 | 5 | 5 |
| **V3** | 4 | 5 | 6 | 4 | 20 |
| **V4** | 20 | 10 | 15 | 15 | 15 |
| **V5** | 20 | 20 | 10 | 15 | 10 |
| **V6** | 15 | 20 | 15 | 20 | 15 |

**Updated risk impacts**

| | **Threat X Vulnerability - Threat exploiting the vulneability** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Assets** | T2* V2 | T2* v3 | T2* V4 | T2* V5 | T2* V6 | T3* V2 | T3* v3 | T3* V4 | T3* V5 | T3* V6 | T4* V2 | T4* v3 | T4* V4 | T4* V5 | T4* V6 | T5* V2 | T5* v3 | T5* V4 | T5* V5 | T5* V6 |
| **A2** | 60 | 50 | 30 | 40 | 50 | 50 | 60 | 30 | 40 | 50 | 50 | 60 | 30 | 50 | 50 | 50 | 60 | 30 | 40 | 50 |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A3** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** |
| **A7** | 50 | 50 | 40 | 30 | 50 | 50 | 60 | 50 | 40 | 50 | 40 | 30 | 30 | 30 | 50 | 30 | 40 | 50 | 40 | 50 |
| **A8** | 40 | 40 | 60 | 40 | 50 | 50 | 30 | 40 | 60 | 50 | 40 | 50 | 30 | 50 | 50 | 30 | 60 | 60 | 40 | 50 |
| **A9** | 60 | 50 | 30 | 40 | 50 | 50 | 60 | 30 | 40 | 50 | 50 | 60 | 30 | 50 | 50 | 50 | 60 | 30 | 40 | 50 |
| **A10** | 30 | 40 | 50 | 30 | 50 | 60 | 30 | 30 | 30 | 50 | 40 | 40 | 50 | 30 | 50 | 60 | 40 | 40 | 30 | 50 |

| | **Threat X Vulnerability - Threat exploiting a vulnerability (All values in percentage)** | | | | |
|---|---|---|---|---|---|
| **Asset** | T6*V2 | T6*v3 | T6*V4 | T6*V5 | T6*V6 |
| A2 | 50 | 50 | 50 | 50 | 50 |
| **A3** | **10** | **10** | **10** | **10** | **10** |
| A7 | 50 | 50 | 50 | 50 | 50 |
| A8 | 50 | 50 | 50 | 50 | 50 |
| A9 | 50 | 50 | 50 | 50 | 50 |
| A10 | 50 | 50 | 50 | 50 | 50 |

## Residual Asset security risks

**Risk of Asset A2:**

500*(5*60+4*50+6*30+5*40 + 15*50+7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50+ 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50) /10 = 592000

**Risk of Asset A3**

950*(5*10+4*10+6*10+5*10+15*10+7*10+5*10+4*10+7*10+20*10+6*10+6*10+8*10+8*10+15*10+5*10+4*10+7*10+4*10+20*10 + 15*10 + 20*10 + 15*10 + 20*10 + 15*10)/10 = 233700

**Risk of Asset A7**

800*(5*50+4*50+6*40+5*30+15*50+7*50+5*60+4*50+7*40+20*50+6*40+6*30+8*30+8*30+15*50+5*30+4*40+7*40+4*40+20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 909600

**Risk of Asset A8**

850*(5*40+4*40+6*60+5*40+15*50+7*50+5*30+4*40+7*60+20*50+6*40+6*50+8*30+8*50+15*50+5*30+4*60+7*60+4*40+20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 1011500

**Risk of Asset A9**

250*(5*60+4*50+6*30+5*40 + 15*50+ 7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50 + 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 296000

**Risk of Asset A10**

300*(5*60+4*50+6*30+5*40 + 15*50+ 7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50 + 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 355200

## Residual vulnerability security risks

**Risk due to V2**

(500*(5*60+7*50+6*50+5*50+5*50) + 950*(5*10+7*10+6*10+5*10+5*10) +
800*(5*50+7*50+6*40+5*30+5*50) +850*(5*40+7*50+6*40+5*30+5*50) +
250*(5*60+7*50+6*50+5*50+5*50) + 300*(5*30+7*60+6*40+5*60+5*50))/10 = 376500

**Risk due to V3**

(500*(4*50+5*60+6*60+4*60+20*50) + 950*(4*10+5*10+6*10+4*10+20*10) +
800*(4*50+5*60+6*30+4*40+20*50) +850*(4*40+5*30+6*50+4*60+20*50) +
250*(4*50+5*60+6*60+4*60+20*50) + 300*(4*40+5*60+6*40+4*40+20*50))/10 = 554800

**Risk due to V4**

(500*(6*30+4*30+8*30+7*30+15*50) + 950*(6*10+4*10+8*10+7*10+15*10) +
800*(6*40+4*50+8*30+7*50+15*50) +850*(6*60+4*40+8*30+7*60+15*50) +
250*(6*30+4*30+8*30+7*30+15*50) + 300*(6*50+4*30+8*50+7*40+15*50))/10 = 512450

**Risk due to V5**

(500*(5*40+7*40+8*50+4*40+10*50) + 950*(5*10+7*10+8*10+4*10+10*10) +
800*(5*30+7*40+8*30+4*40+10*50) +850*(5*40+7*60+8*50+4*40+10*50) +
250*(5*40+7*40+8*50+4*40+10*50) + 300*(5*30+7*30+8*30+4*30+10*50))/10 = 433600

**Risk due to V6**

(500*(15*50+20*50+15*50+20*50+15*50) + 950*(15*10+20*10+15*10+20*10+15*10) +
800*(15*50+20*50+15*50+20*50+15*50) +850*(15*50+20*50+15*50+20*50+15*50) +
250*(15*50+20*50+15*50+20*50+15*50) + 300*(15*50+20*50+15*50+20*50+15*50))/10 =
1228250

## Ranking of security asset residual risk

| Asset | Residual risk | Rank |
|---|---|---|
| **A8** | **101150** | **1** |
| **A7** | 90960 | 2 |
| **A2** | 59200 | 3 |
| **A10** | 35520 | 4 |
| **A9** | 29600 | 5 |
| **A3** | 23370 | 6 |

## Ranking of vulnerability security risks

| Vulnerability | Vulnerability security risk | Rank |
|---|---|---|
| **V6** | 1228250 | 1 |
| **V3** | 554800 | 2 |
| **V4** | 512450 | 3 |
| **V5** | 433600 | 4 |

| | | |
|---|---|---|
| **V2** | 376500 | 5 |

## Security risk response strategy R3

Apply additional Hardening Controls to new now highest ranked Residual Asset Risk, thus reducing risk impact probabilities, and further reducing the overall security asset residual risk and create a new ranking of vulnerability security risks. In this step you 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).

We see that asset A8 - Reputation has the highest residual risk according to calculations in R1. Reputation is an extremely important factor for any organization. However good the products/services of an organization are, it's always important to have measures that protect the organization's reputation. Reputation can be improved by submitting the right payroll documents and employee records.

## Threat Vulnerabilities pairs on asset subset - A2,A3,A7,A8,A9,A10

| | **T2** | **T3** | **T4** | **T5** | **T6** |
|---|---|---|---|---|---|
| **V2** | 5 | 7 | 6 | 5 | 5 |
| **V3** | 4 | 5 | 6 | 4 | 20 |
| **V4** | 20 | 10 | 15 | 15 | 15 |
| **V5** | 20 | 20 | 10 | 15 | 10 |
| **V6** | 15 | 20 | 15 | 20 | 15 |

## Updated risk impacts

| | **Threat X Vulnerability - Threat exploiting the vulneability** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Assets** | T2* V2 | T2* v3 | T2* V4 | T2* V5 | T2* V6 | T3* V2 | T3* v3 | T3* V4 | T3* V5 | T3* V6 | T4* V2 | T4* v3 | T4* V4 | T4* V5 | T4* V6 | T5* V2 | T5* v3 | T5* V4 | T5* V5 | T5* V6 |
| **A2** | 60 | 50 | 30 | 40 | 50 | 50 | 60 | 30 | 40 | 50 | 50 | 60 | 30 | 50 | 50 | 50 | 60 | 30 | 40 | 50 |
| **A3** | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| **A7** | 50 | 50 | 40 | 30 | 50 | 50 | 60 | 50 | 40 | 50 | 40 | 30 | 30 | 30 | 50 | 30 | 40 | 50 | 40 | 50 |

| | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **A8** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** | **10** |
| **A9** | 60 | 50 | 30 | 40 | 50 | 50 | 60 | 30 | 40 | 50 | 50 | 60 | 30 | 50 | 50 | 50 | 60 | 30 | 40 | 50 |
| **A10** | 30 | 40 | 50 | 30 | 50 | 60 | 30 | 30 | 30 | 50 | 40 | 40 | 50 | 30 | 50 | 60 | 40 | 40 | 30 | 50 |

| | **Threat X Vulnerability - Threat exploiting a vulnerability (All values in percentage)** | | | | |
|---|---|---|---|---|---|
| **Asset** | T6*V2 | T6*v3 | T6*V4 | T6*V5 | T6*V6 |
| A2 | 50 | 50 | 50 | 50 | 50 |
| **A3** | 10 | 10 | 10 | 10 | 10 |
| A7 | 50 | 50 | 50 | 50 | 50 |
| A8 | **10** | **10** | **10** | **10** | **10** |
| A9 | 50 | 50 | 50 | 50 | 50 |
| A10 | 50 | 50 | 50 | 50 | 50 |

**Calcualte Residual Asset security risks**

**Risk of Assest A2:**

500*(5*60+4*50+6*30+5*40 + 15*50+7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50+ 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50) /10 = 59200

**Risk of Asset A3**

950*(5*10+4*10+6*10+5*10+15*10+7*10+5*10+4*10+7*10+20*10+6*10+6*10+8*10+8*10+15*10+5*10+4*10+7*10+4*10+20*10 + 15*10 + 20*10 + 15*10 + 20*10 + 15*10)/10 = 23370

**Risk of Asset A7**

800*(5*50+4*50+6*40+5*30+15*50+7*50+5*60+4*50+7*40+20*50+6*40+6*30+8*30+8*30+15*50+5*30+4*40+7*40+4*40+20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 90960

**Risk of Asset A8**

850*(5*10+4*10+6*10+5*10+15*10+7*10+5*10+4*10+7*10+20*10+6*10+6*10+8*10+8*10+15*10+5*10+4*10+7*10+4*10+20*10 + 15*10 + 20*10 + 15*10 + 20*10 + 15*10)/10 = 20910

**Risk of Asset A9**

250*(5*60+4*50+6*30+5*40 + 15*50+ 7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50 + 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 29600

**Risk of Asset A10**

300*(5*60+4*50+6*30+5*40 + 15*50+ 7*50+5*60+4*30+7*40+20*50 + 6*50+6*60+8*30+8*50 + 15*50+5*50+4*60+7*30+4*40 + 20*50 + 15*50 + 20*50 + 15*50 + 20*50 + 15*50)/10 = 355200

## Residual vulnerability security risks

**Risk due to V2**

(500*(5*60+7*50+6*50+5*50+5*50) + 950*(5*10+7*10+6*10+5*10+5*10) +
800*(5*50+7*50+6*40+5*30+5*50) +850*(5*10+7*10+6*10+5*10+5*10) +
250*(5*60+7*50+6*50+5*50+5*50) + 300*(5*30+7*60+6*40+5*60+5*50))/10 = 299150

**Risk due to V3**

(500*(4*50+5*60+6*60+4*60+20*50) + 950*(4*10+5*10+6*10+4*10+20*10) +
800*(4*50+5*60+6*30+4*40+20*50) +850*(4*10+5*10+6*10+4*10+20*10) +
250*(4*50+5*60+6*60+4*60+20*50) + 300*(4*40+5*60+6*40+4*40+20*50))/10 = 430700

**Risk due to V4**

(500*(6*30+4*30+8*30+7*30+15*50) + 950*(6*10+4*10+8*10+7*10+15*10) +
800*(6*40+4*50+8*30+7*50+15*50) +850*(6*10+4*10+8*10+7*10+15*10) +
250*(6*30+4*30+8*30+7*30+15*50) + 300*(6*50+4*30+8*50+7*40+15*50))/10 = 382400

**Risk due to V5**

(500*(5*40+7*40+8*50+4*40+10*50) + 950*(5*10+7*10+8*10+4*10+10*10) +
800*(5*30+7*40+8*30+4*40+10*50) +850*(5*40+7*10+8*10+4*10+10*10) +
250*(5*40+7*40+8*50+4*40+10*50) + 300*(5*30+7*30+8*30+4*30+10*50))/10 = 332450

**Risk due to V6**

(500*(15*50+20*50+15*50+20*50+15*50) + 950*(15*10+20*10+15*10+20*10+15*10) +
800*(15*50+20*50+15*50+20*50+15*50) +850*(15*10+20*10+15*10+20*10+15*10) +

250*(15*50+20*50+15*50+20*50+15*50) + 300*(15*50+20*50+15*50+20*50+15*50))/10 = 939250

## Ranking of security asset residual risk

| Asset | Residual risk | Rank |
|---|---|---|
| **A7** | 90960 | 1 |
| **A2** | 59200 | 2 |
| **A10** | 35520 | 3 |
| **A9** | 29600 | 4 |
| **A3** | 23370 | 5 |
| **A8** | 20910 | 6 |

## Ranking of vulnerability security risks

| Vulnerability | Vulnerability security risk | Rank |
|---|---|---|
| **V6** | 939250 | 1 |
| **V3** | 430700 | 2 |
| **V4** | 382400 | 3 |
| **V5** | 332450 | 4 |
| **V2** | 299150 | 5 |

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

All the controls listed were part of the 157 risk controls in the common criteria such as contingency planning, configuration management, incident response, awareness and training. List also included technical security controls such as access control and system and communication protection.

## Mixed Security risk prevention strategy

This strategy uses the techniques of P3 and R3 combined to reduce the risk of assets and vulnerabilities even further. Most of the real world organizations apply a combination of preventive and responsive strategies. Both the strategies need not have the same weightage but its important to have a combination of both. Here we are using the preventive strategy P3 that involves improving the contingency planning and responsive strategy R3 that involves safeguarding the personal information by using better encryption techniques and secure databases.

Threat vulnerabilities pairs updated after P3 and R3

| | **T2** | **T3** | **T4** | **T5** | **T6** |
|---|---|---|---|---|---|
| **V2** | 5 | 7 | 6 | 5 | 5 |
| **V3** | 4 | 5 | 6 | 4 | 5 |
| **V4** | 6 | 4 | 8 | 7 | 5 |
| **V5** | 5 | 7 | 8 | 4 | 5 |
| **V6** | 5 | 7 | 6 | 5 | 5 |

**Updated risk impacts**

| | **Threat X Vulnerability - Threat exploiting the vulneability** | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| **Assets** | T2* V2 | T2* v3 | T2* V4 | T2* V5 | T2* V6 | T3* V2 | T3* v3 | T3* V4 | T3* V5 | T3* V6 | T4* V2 | T4* v3 | T4* V4 | T4* V5 | T4* V6 | T5* V2 | T5* v3 | T5* V4 | T5* V5 | T5* V6 |
| **A2** | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| **A3** | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| **A7** | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| **A8** | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| **A9** | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |
| **A10** | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 | 10 |

| | **Threat X Vulnerability - Threat exploiting a vulnerability (All values in percentage)** | | | | |
|---|---|---|---|---|---|
| **Asset** | T6*V2 | T6*v3 | T6*V4 | T6*V5 | T6*V6 |
| A2 | 10 | 10 | 10 | 10 | 10 |
| **A3** | 10 | 10 | 10 | 10 | 10 |
| A7 | 10 | 10 | 10 | 10 | 10 |
| A8 | 10 | 10 | 10 | 10 | 10 |

| | | | | | |
|---|---|---|---|---|---|
| A9 | 10 | 10 | 10 | 10 | 10 |
| A10 | 10 | 10 | 10 | 10 | 10 |

**Calcualte Residual Asset security risks**

**Risk of Assest A2:**

500*(5*10+4*10+6*10+5*10+5*10+7*10+5*10+4*10+7*10+7*10+6*10+6*10+8*10+8*10+6*10+5*10+4*10+7*10+4*10+5*10 + 5*10 + 5*10 + 5*10 + 5*10 + 5*10) /10 = 6950

**Risk of Asset A3**

950*(5*10+4*10+6*10+5*10+5*10+7*10+5*10+4*10+7*10+7*10+6*10+6*10+8*10+8*10+6*10+5*10+4*10+7*10+4*10+5*10 + 5*10 + 5*10 + 5*10 + 5*10 + 5*10)/10 = 13205

**Risk of Asset A7**

800*(5*10+4*10+6*10+5*10+5*10+7*10+5*10+4*10+7*10+7*10+6*10+6*10+8*10+8*10+6*10+5*10+4*10+7*10+4*10+5*10 + 5*10 + 5*10 + 5*10 + 5*10 + 5*10)/10 = 11120

**Risk of Asset A8**

850*(5*10+4*10+6*10+5*10+5*10+7*10+5*10+4*10+7*10+7*10+6*10+6*10+8*10+8*10+6*10+5*10+4*10+7*10+4*10+5*10 + 5*10 + 5*10 + 5*10 + 5*10 + 5*10)/10 = 11815

**Risk of Asset A9**

250*(5*10+4*10+6*10+5*10+5*10+7*10+5*10+4*10+7*10+7*10+6*10+6*10+8*10+8*10+6*10+5*10+4*10+7*10+4*10+5*10 + 5*10 + 5*10 + 5*10 + 5*10 + 5*10)/10 = 3475

**Risk of Asset A10**

300*(5*10+4*10+6*10+5*10+5*10+7*10+5*10+4*10+7*10+7*10+6*10+6*10+8*10+8*10+6*10+5*10+4*10+7*10+4*10+5*10 + 5*10 + 5*10 + 5*10 + 5*10 + 5*10)/10 = 4170

**Calcualte residual vulnerability security risks**

**Risk due to V2**

(500*(5*10+7*10+6*10+5*10+5*10) + 950*(5*10+7*10+6*10+5*10+5*10) +
800*(5*10+7*10+6*10+5*10+5*10) +850*(5*10+7*10+6*10+5*10+5*10) +
250*(5*10+7*10+6*10+5*10+5*10) + 300*(5*10+7*10+6*10+5*10+5*10))/10 = 102200

**Risk due to V3**

(500*(4*10+5*10+6*10+4*10+5*10) + 950*(4*10+5*10+6*10+4*10+5*10) +
800*(4*10+5*10+6*10+4*10+5*10) +850*(4*10+5*10+6*10+4*10+5*10) +
250*(4*10+5*10+6*10+4*10+5*10) + 300*(4*10+5*10+6*10+4*10+5*10))/10 = 87600

**Risk due to V4**

(500*(6*10+4*10+8*10+7*10+5*10) + 950*(6*10+4*10+8*10+7*10+5*10) +
800*(6*10+4*10+8*10+7*10+5*10) +850*(6*10+4*10+8*10+7*10+5*10) +
250*(6*10+4*10+8*10+7*10+5*10) + 300*(6*10+4*10+8*10+7*10+5*10))/10 = 109500

**Risk due to V5**

(500*(5*10+7*10+8*10+4*10+5*10) + 950*(5*10+7*10+8*10+4*10+5*10) +
800*(5*10+7*10+8*10+4*10+5*10) +850*(5*10+7*10+8*10+4*10+5*10) +
250*(5*10+7*10+8*10+4*10+5*10) + 300*(5*10+7*10+8*10+4*10+5*10))/10 = 105850

**Risk due to V6**

(500*(5*10+7*10+6*10+5*10+5*10) + 950*(5*10+7*10+6*10+5*10+5*10) +
800*(5*10+7*10+6*10+5*10+5*10) +850*(5*10+7*10+6*10+5*10+5*10) +
250*(5*10+7*10+6*10+5*10+5*10) + 300*(5*10+7*10+6*10+5*10+5*10))/10 = 102200

## Ranking of security asset residual risk

| Asset | Residual risk | Rank |
|---|---|---|
| **A3** | 13205 | 1 |
| **A8** | 11815 | 2 |
| **A7** | 11120 | 3 |

| | | |
|---|---|---|
| **A2** | 6950 | 4 |
| **A10** | 4170 | 5 |
| **A9** | 3475 | 6 |

## Ranking of vulnerability security risks

| Vulnerability | Vulnerability security risk | Rank |
|---|---|---|
| **V4** | 109500 | 1 |
| **V5** | 105850 | 2 |
| **V2** | 102200 | 3 |
| **V6** | 102200 | 4 |
| **V3** | 87600 | 5 |

**Estimate a Risk Prevention budget, a Risk Response budget, and a mixed strategy budget.**

| Controls | Risk Prevention budget | Risk Response budget | Mixed strategy budget |
|---|---|---|---|
| Mitigating Vulnerabilities Related to Payroll Fraud | $200,000 | $250,000 | $300,000 |
| Mitigating Payroll Error | $100,000 | $100,000 | $150,000 |
| Mitigating Vulnerabilities Related to Continuity of Operations | $300,000 | $400,000 | $500,000 |
| Mitigating Vulnerabilities | $250,000 | $300,000 | $400,000 |

| | | | |
|---|---|---|---|
| Related to Disclosure or Brokerage of information | | | |
| Mitigating Vulnerabilities Related to NetworkRelated Attacks | $400,000 | $300,000 | $500,000 |
| Addition of VPN | $100,000 | $150,000 | $200,000 |
| Addition of DMZ | $200,000 | $100,000 | $300,000 |
| **Total** | **$1,550,000** | **$1,600,000** | **$2,450,000** |

## Conclusion: Cost-Benefit Analysis

HGA's risk management recommendations were thorough and detailed. The entire organization was systematically divided to find all the assets, vulnerabilities, and threats. Focusing on critical assets was the key factor in managing risk effectively. Accurate and actionable tasks were suggested to bring the risk down.

MOT model was used by HGA effectively. MOT model allows us to categorize the recommendations effectively and balance the effort so that all use cases are covered. Various controls in all the three categories were provided. Management controls included - security audits, duties segregation, etc. Operational audits included - security awareness training, backups etc. and Technical controls included - access control, data redundancy

Risk Preventive vs Response vs Mixed strategies - In today's age of cybersecurity, its is almost close to impossible to prevent all security threats. Cyber security is a cat and mouse game. Attackers and defenders always play catch-up between each other. Using only preventive or only response strategy is not going to protect any organization from all the cyber threats. From my experience of working in a major cybersecurity firm - risk management must always be a combination of preventive and response strategies. That gives any organization a best chance

of fighting cyber threats. As discussed in class - they maynot always get the same effort or resources but both of them needs to addressed even if one of them accounts only 10% of total resources.

**Cost-benefit ratio analysis for Risk Prevention budget**

Total Asset value for chosen assets = $3,650,000
Total Residual risk for assets after implementing risk analysis = $1,095,000
Expected Security risk-benefit = $2,555,000

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 1,550,000/2,555,000
  = 0.606

**Cost-benefit ratio analysis for Risk Response budget**

Total Asset value for chosen assets = $3,650,000
Total Residual risk for assets after implementing risk analysis = $229,960
Expected Security risk-benefit = $3,420,040

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 1,600,000/3,420,040
  = 0.468

**Cost-benefit ratio analysis for Mixed strategy budget**

Total Asset value for chosen assets = $3,650,000
Total Residual risk for assets after implementing risk analysis = $50,735
Expected Security risk-benefit = $3,599,265

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 2,450,000/3,599,265
  = 0.681

# Part B

## 1. Access Control Security Risk Management Implementation Controls and Policies

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

**List of critical assets**

| Asset | Approximate dollar value |
|---|---|
| Employees and customer PII | $50,000,000 |
| Source code and software | $30,000,000 |
| Financial resources | $20,000,000 |
| Email server | $60,000,000 |
| Reputation | $70,000,000 |

**List of missing controls**

- Static routes for sensitive data transfer
- Backdoor connections
- Hybrid technology firewall
- Application proxy firewall
- Secure router planes

**List of potential vulnerabilities for critical assets**

- Unauthorized access
- Bugs in source code and software
- Unauthorized access
- Administrative access to modify the mail server
- Disgruntled employee

**List of potential threats that could exploit the vulnerabilities for critical assets**

- Leaked PII data
- Ransomware
- Remote code execution
- Disabling or crashing the system
- Leaked confidential financial data
- DOS threats
- Leaked confidential emails
- Leaking confidential company data
- Whistleblowers

**List of security risks**

- Information disclosure
- Data integrity
- Malware execution
- Denial of Service
- Leaked confidential financial data
- Leaked confidential emails
- Leaking confidential company data
- Insider threat

**2. Network Infrastructure Security Risk Management Implementation Controls and Policies**

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

**List of critical assets**

| Asset | Approximate dollar value |
|---|---|
| Employees and customer PII | $50,000,000 |
| Source code and software | $30,000,000 |
| Financial resources | $20,000,000 |
| Email server | $60,000,000 |
| Reputation | $70,000,000 |

**List of missing controls**

- Static routes for sensitive data transfer
- Backdoor connections
- Hybrid technology firewall
- Application proxy firewall
- Secure router planes

**List of potential vulnerabilities for critical assets**

- Unauthorized access
- Bugs in source code and software
- Unauthorized access
- Administrative access to modify the mail server
- Disgruntled employee

**List of potential threats that could exploit the vulnerabilities for critical assets**

- Leaked PII data
- Ransomware
- Remote code execution
- Disabling or crashing the system
- Leaked confidential financial data
- DOS threats
- Leaked confidential emails

- Leaking confidential company data
- Whistleblowers

**List of security risks**

- Information disclosure
- Data integrity
- Malware execution
- Denial of Service
- Leaked confidential financial data
- Leaked confidential emails
- Leaking confidential company data
- Insider threat

## 3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies

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

**List of critical assets**

| **Asset** | **Approximate dollar value** |
|---|---|
| Employees and customer PII | $50,000,000 |
| Source code and software | $30,000,000 |

| | |
|---|---|
| Financial resources | $20,000,000 |
| Email server | $60,000,000 |
| Reputation | $70,000,000 |

**List of missing controls**

- Static routes for sensitive data transfer
- Backdoor connections
- Hybrid technology firewall
- Application proxy firewall
- Secure router planes

**List of potential vulnerabilities for critical assets**

- Unauthorized access
- Bugs in source code and software
- Unauthorized access
- Administrative access to modify the mail server
- Disgruntled employee

**List of potential threats that could exploit the vulnerabilities for critical assets**

- Leaked PII data
- Ransomware
- Remote code execution
- Disabling or crashing the system
- Leaked confidential financial data
- DOS threats
- Leaked confidential emails
- Leaking confidential company data
- Whistleblowers

**List of security risks**

- Information disclosure
- Data integrity
- Malware execution
- Denial of Service
- Leaked confidential financial data
- Leaked confidential emails
- Leaking confidential company data
- Insider threat

## 4. Database Security Risk Management Implementation Controls and Policies

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

**List of critical assets**

| **Asset** | **Approximate dollar value** |
|---|---|
| Employees and customer PII | $50,000,000 |
| Source code and software | $30,000,000 |

| | |
|---|---|
| Financial resources | $20,000,000 |
| Email server | $60,000,000 |
| Reputation | $70,000,000 |

**List of missing controls**

- Static routes for sensitive data transfer
- Backdoor connections
- Hybrid technology firewall
- Application proxy firewall
- Secure router planes

**List of potential vulnerabilities for critical assets**

- Unauthorized access
- Bugs in source code and software
- Unauthorized access
- Administrative access to modify the mail server
- Disgruntled employee

**List of potential threats that could exploit the vulnerabilities for critical assets**

- Leaked PII data
- Ransomware
- Remote code execution
- Disabling or crashing the system
- Leaked confidential financial data
- DOS threats
- Leaked confidential emails
- Leaking confidential company data
- Whistleblowers

**List of security risks**

- Information disclosure
- Data integrity
- Malware execution
- Denial of Service
- Leaked confidential financial data
- Leaked confidential emails
- Leaking confidential company data
- Insider threat

## 5. Applications Development Security Risk Management Implementation Controls and Policies

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

**List of critical assets**

| **Asset** | **Approximate dollar value** |
|---|---|
| Employees and customer PII | $50,000,000 |
| Source code and software | $30,000,000 |
| Financial resources | $20,000,000 |
| Email server | $60,000,000 |
| Reputation | $70,000,000 |

**List of missing controls**

- Static routes for sensitive data transfer
- Backdoor connections
- Hybrid technology firewall
- Application proxy firewall
- Secure router planes

**List of potential vulnerabilities for critical assets**

- Unauthorized access
- Bugs in source code and software
- Administrative access to modify the mail server
- Disgruntled employee

**List of potential threats that could exploit the vulnerabilities for critical assets**

- Leaked PII data
- Ransomware
- Remote code execution
- Disabling or crashing the system
- Leaked confidential financial data
- DOS threats
- Leaked confidential emails
- Leaking confidential company data
- Whistleblowers

**List of security risks**

- Information disclosure
- Data integrity
- Malware execution
- Denial of Service
- Leaked confidential financial data

- Leaked confidential emails
- Leaking confidential company data
- Insider threat

## 6. Wireless Security Risk Management Implementation Controls and Policies

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

**List of critical assets**

| **Asset** | **Approximate dollar value** |
|---|---|
| Employees and customer PII | $50,000,000 |
| Source code and software | $30,000,000 |
| Financial resources | $20,000,000 |
| Email server | $60,000,000 |
| Reputation | $70,000,000 |

**List of missing controls**

- Static routes for sensitive data transfer
- Backdoor connections
- Hybrid technology firewall
- Application proxy firewall
- Secure router planes

**List of potential vulnerabilities for critical assets**

- Unauthorized access
- Bugs in source code and software
- Unauthorized access
- Administrative access to modify the mail server
- Disgruntled employee

**List of potential threats that could exploit the vulnerabilities for critical assets**

- Leaked PII data
- Ransomware
- Remote code execution
- Disabling or crashing the system
- Leaked confidential financial data
- DOS threats
- Leaked confidential emails
- Leaking confidential company data
- Whistleblowers

**List of security risks**

- Information disclosure
- Data integrity
- Malware execution
- Denial of Service
- Leaked confidential financial data
- Leaked confidential emails
- Leaking confidential company data
- Insider threat

7. Across all Security Risk areas 1-6 from above provide a table for:

a) List of Cybersecurity Implementation controls that exist at Secure Systems

**1. Access Control Security Risk Management Implementation Controls and Policies**

**Identification Controls**

ID card / Employee badge – To enter or leave the office premises
Email/username and password – To access email and other internal resources

**Personal Authentication**

Password – Typically a password for the email IDs and corporate IDs
Employee badge/ID card – To enter or leave the office premises
Duo two-factor authentication- To access critical internal resources

**Authorization**

Access to specific assets such as:
Physical Assets - Control rooms, IT security rooms was maintained by the security operations center
Logical Assets - Networks, applications, services were maintained by the IT operations team

**Logical Access Control methods**

Network access control - Network access in the office was protected by username and password with 2FA
Remote network access – Remote employees were allowed to access internal resources only with VPN
Encryption – All the data stored and transmitted was encrypted

**Physical access control**

Classified storage and handling – Authorized individuals based on their badge were allowed to access classified storage and handling
Attended access for guests – All guests must sign in with their details before entering the office

**2. Network Infrastructure Security Risk Management Implementation Controls and Policies**

**Enclave Protection**

Packet filtering router/firewall - To filter packets based on protocol, IP, flags
Demilitarized zone - To separate external-facing resources with internal critical resources
Restricted LAN segment - To be used for critical resources like AD, FTP, internal DNS services

**Firewall**

Packet filtering firewall - To filter packets based on protocol, IP, flags
Bastion host - Extremely secure system used just for firewalls
Stateful inspection - Layer 4 awareness to packet filtering firewalls
Deep packet inspection - To check for IDS signatures for harmful traffic

**Routers**

Router table integrity - Ensuring the correctness of routing table in routers
Securing router planes - Ensures insecure protocols/applications can communicate securely over a network

3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies

**Ports, protocols, and services**

ICMPv4 messages - To block echo request and reply to stop an attacker from creating a network map
DDOS agents - To block particular ports and use automated scanning tools
IPV4 address filtering - To filter traffic flowing in and out of the organization's network
IPV6 address filtering - To filter traffic using IPV6 address notation.
SYN flood attack protection - To protect LANs, servers, and routers from SYN flood attacks by using various techniques such as redundancy and SYN cookies

**Network Authentication, Authorization, and Accounting**

Accounts - Individual and group accounts with passwords must be setup and audited
Local Accounts - Local accounts will default to the lowest authorization level
Auditing - System auditing can be done with the help of Syslog and the logs have to be encrypted as well
Router password protection - Routers have to be protected by passwords with reasonable encryption

**Network Intrusion Detection Systems**

LAN intrusion detection - Host IDS combined with enclave protection can give us alarms for network-based attacks on the company LAN
External network intrusion detection - External NIDS is typically installed in front of the premise or border router can give us the details about external threat vectors

**Switches and VLAN**

Switches and Wiring - Physical security of the wires must be done with the help of secured IDF
VLAN access and port authentication - To disable ports into an unused VLAN thereby preventing unauthorized access
VLAN 802.1x and management policy server - To limit network access based on client profile

**VPN**

Host-to-gateway - Allowing external hosts to establish VPN connections to the gateway of the organization

4. Database Security Risk Management Implementation Controls and Policies

**Authentication - user accounts**

Different users such as application user, database administrator, application owner, database operator, and database auditor are created for the implementation of separation of privileges

**Authorization**

- RBAC is implemented for separation of duties and the principle of least privilege.
- Single or multiple DB accounts can be used based on the use case.

**Confidentiality**

- Encryption is used to store critical data in rest and transit.
- Source code needs to be encrypted or encoded

**Integrity**

Transaction logs need to be encrypted to help protect data integrity against inconsistencies.

**Back up and recovery**

- Due to the sensitivity of DB recovery, testing these systems is very important.
- Backup data needs to be protected with encryption and access control.

**OS protection**

- Use trusted vendors and OS for critical systems.
- Security patches need to be installed as quickly as possible to avoid any known vulnerabilities.

**Application protection**

- Authentication method of the application connecting to the database needs to be reviewed thoroughly.
- The principle of least privilege has to be implemented for applications accessing the DB

**Network protection**

- Determine which users/systems need remote access
- Use VPN and IDS wherever necessary to complement OS and application protection techniques.

**Business continuity**

- Backup and restoration assets need to be protected.
- Disaster and recovery planning should be included with the overall site plan.

**Vulnerability and incident management**

- DBMS software needs to be updated and patched when supported by the vendor
- Trusted and supported versions need to be used

5. Applications Development Security Risk Management Implementation Controls and Policies

**Application data handling**

- FIPS 140-2 and NSA-approved type-1 encryption should be used.
- Data at rest and data in transit should be encrypted as well.
- Data integrity should be maintained using parity checks and CRCs

**Authentication**

- A combination of user and/or server authentication must be implemented
- Standalone and components of applications must also be authenticated

**Use of cryptography**

- Symmetric ciphers to protect confidential data.
- Message authentication codes and digital signatures can also be used.

**User accounts**

- Unnecessary accounts should be disabled or deleted by default
- Lockout policies on incorrect password attempts should be implemented to prevent brute-forcing.

**Input validation**

- Static analysis tools should be used to find vulnerabilities.
- Validate all input - good and bad before being used to the best of your abilities.

**Auditing**

- Capability to notify user logins with details such as time, date, userID, etc.
- Content of audit trails should be protected against unauthorized access.

**Configuration Management**

- System software must be approved by the config control board
- Software config management process will limit unauthorized access to source code.

**Testing**

- Fuzz testing can be used to test all possible inputs.
- Automated tools can be used to reduce manual effort.

**Deployment**

- All deployment processes must be well documented.
- Applications maintenance for vulnerability and availability is important.

6. Wireless Security Risk Management Implementation Controls and Policies

**Wireless LAN Risk Management**

- SSL iis used for all secure communications
- WPA3 is implemented for all the Wi-Fi networks.
- VPN tunneling can be used for accessing internal resources for remote workers

**Wireless PAN Risk Management**

- Bluetooth 4.X is used to prevent known vulnerabilities in older versions
- CIAA security principles must be applied for Bluetooth connections as well.
- Wireless mice and keyboards must be avoided in high-security situations

**Wireless WAN Risk Management**

- Cellular Digital Packet Data (CDPD) standard must be used to provide device-level authentication and data encryption.
- Device-level authentication can be used but it is vulnerable to cloning problems

**Wireless RFID Risk Management**

There arent any details about RFID risk management as the orgaination is not using any RFID devices for business puposes

**Wireless PED Risk Management**

- SMS protocol provides no security features.
- SIM card functions are now enhanced and provide authentication, encryption, and data storage.
- GSM provides type1-4 encryption with PIN access.

b) Comparison of the Implementation controls discussed in class with Secure Systems's existing
Cybersecurity Implementation controls

**1. Access Control Security Risk Management Implementation Controls and Policies**

Identification controls listed in the slides is the same as the ones implemented in the company

Personal authentication controls remain more or less the same. They are specific password policies and Duo is used for 2FA

Authorization controls are similar as well. There are specific authorizations for specific employees both for physical and logical assets.

Logical access control methods are similar to what was discussed in class. Each team has only access to the resources they need to complete their job effectively. Network access control is implemented effectively so that in the company network, you don't have to authenticate yourself again.

Physical access control methods are similar to what was listed in the slides. There were rooms/workspaces that not all employees had access to. Such as IT security rooms. Any guests had to sign and should always be accompanied by an employee.

Biometric systems were not implemented in my previous organization

**2. Network Infrastructure Security Risk Management Implementation Controls and Policies**

**Enclave Protection**

Packet filtering firewall is implemented to act as a first-level filter to avoid unnecessary traffic in a easy and scalable format.
DMZ is implemented to separate external and internal services to provide defense in depth security.
Restricted LAN segments are used when there is a need to test malware and it should be separated from the corporate network.

Static routes are typically not used as this is not a federal government agency or a contractor for the federal government.
Backdoor connections are typically avoided to not open up any security loopholes.

**Firewall**

Packet filtering firewall with typically bastion host is used across many divisions in the company to avoid any single point of failure.
Deep packet inspection is used to implement IDS signature for malware analysis and other network attacks
Stateful inspection firewall is used to complement the complement the packet filtering firewall with bastion host.

**Routers**

Router table integrity is implemented by using specific router protocols and also using neighbor router authentication. SHA-2 or IPsec is typically used for this purpose.
Router planes are secured by using fully patched operating systems, Cisco Delivery Protocols and sometimes IPv6

3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies

**Ports, protocols, and services**

Red/Yellow/Green ports are confidential to the company's policies and that is not described here. ICMP ping requests and traceroute to identify organizations network is blocked for external IPs. Firewalls to filter IPV4 and IPV6 traffic is implemented as part of the company's SOC policies. SYN flood protection is implemented as well.

**Device Management** and **Device Monitoring** details are not available.

### Network Authentication, Authorization, and Accounting

AAA policies are extremely important as it's not easy to manage new employees coming to the organization and employees leaving the organization. Employees leaving the organization have to be revoked access and their accounts need to be deleted accordingly. Regular auditing is done on the organization's network logs to monitor for any discrepancies.

### Network Intrusion Detection Systems

IDS plays a key role in detecting and mitigating attacks on organizations' networks. Both internal IDS and external IDS were implemented to keep track of external threat vectors and mitigate them.

### Switches and VLAN

VLAN were a critical part of the organizations' network because there were many sections of employees in the organization - developers, managers, sales reps, and so on. It is important to have them in specific VLANs so that they have the right access to the resources they need and also provide logical network separation.

### VPN

VPN was a critical part of the organization's network infrastructure because of the pandemic. Most of the employees were working remotely and the VPN server was designed to handle the load and security of the internal resources from attackers. Cisco AnyConnect VPN with 2FA was implemented to provide host-to-gateway VPN access.

## 4. Database Security Risk Management Implementation Controls and Policies

### Authentication and Authorization

All the employees accessing the databases in the company have specific roles and use cases. They can be either a user or administrator or manager and so on. There are teams that take

care of assigning these privileges. The principle of least privilege is implemented in database access. RBAC is widely used across the organization.

**Confidentiality**

Encryption is a key component in ensuring the confidentiality of sensitive data both in rest and 61transit. Source code is one of the key assets of the organization I was working with. Best in class, industry-standard encryption algorithms are used and updated regularly for encryption.

**Integrity**

Providing integrity of data including transaction logs is an extremely important factor in the organization's success. These transaction logs are encrypted in transit and are monitored using an automated system for inconsistencies.

**Back up and recovery**

Backup and recovery are an essential part of the business continuity plan of the organization. Automated backup with regular testing is implemented to safeguard against unknown threats to the database.

**OS protection**

OS protection is extremely important because most of the vulnerabilities that are exploited are known vulnerabilities in the OS or the database. Zero-days are very rare and keeping the OS and the DB software up-to-date with the latest and greatest security patches is not just important but essential.

**Application protection**

All users accessing the DB application is authenticated and should be in the company's internal network. If they are working remotely, they need to be on a VPN to access these resources. The principle of least privilege is used for applications accessing the DB to prevent any privilege escalation attacks.

**Network protection**

Complimenting all other protections, network protection adds an extra layer of security to the database. A VPN is used for users accessing the database remotely. IDS is used to keep track of data flowing through the network.

**Vulnerability and incident management**

Vulnerabilities and incidents are not going to stop anytime soon. It's important to have teams that can effectively manage reported vulnerabilities, implement security patches, and handle security incidents in the company. It's always preferable to use trusted and supported DB software and trusted OS for sensitive and critical data.

5. Applications Development Security Risk Management Implementation Controls and Policies

**Application data handling**

Data used by the applications are always encrypted with industry standard encryption practices. Data stored in the database systems is always encrypted as well. Passwords are hashed with one way hashing functions. Data in protected in transit and at rest.

**Authentication**

User and server authentication is performed using PKI - public key infrastructure. Source code used for development of applications is always signed and validated before being used.

**Use of cryptography**

A combination of symmetric and asymmetric ciphers are used in various parts of the organization based on the use case. Digital signatures are widely used for data authentication.

**User accounts**

Maintaining user accounts is an important part of keeping the organization safe. Regular password change policies and 2FA can keep the account secure from being compromised.

**Input validation**

All the applications have thorough input validation to prevent vulnerability such as SQL injections, buffer overflows and command injections.

**Auditing**

All the applications have detailed logging policies which record plethora of information including but not limited to - userID, event, timestamps, start and end time, etc.

**Testing**

Extensive testing of the products is done before being released to the customers. Fuzzing, code reviews, automated tools are widely used all across the organization to ensure the quality of the products in not compromised in any way.

**Deployment**

Usually the last stage of the SDLC, but one of the most important stages. Detailed and thorough documentation of the product including security plans, third party software integration is taken care here.

6. Wireless Security Risk Management Implementation Controls and Policies

**Wireless LAN Risk Management**

All the communication between the devices is encrypted using SSL. WPA3 is used for Wi-Fi authentication for the devices. VPNs are used extensively as many employees are working from home and need to access internal resources of the organization.

**Wireless PAN Risk Management**

There aren't many guidelines provided by the organization on the type of Bluetooth devices to be used and their versions. But employees are always encouraged to use the latest and greatest version of drivers and software's installed in the laptops provided by the organization.

**Wireless WAN Risk Management**

There aren't any guidelines provided by the organization on WAN risk management.

**Wireless RFID Risk Management**

There aren't any details about RFID risk management as the organization is not using any RFID devices for business purposes

**Wireless PED Risk Management**

Organization does not provide personal devices such as phone or sims to the employees. Laptops provided are encrypted and can only be opened by the employee who is assigned with that lab and administrator. Personal devices shouldn't be used for communication of important messages regrading either in SMS or on calls.

c) List of critical assets that exist in Secure Systems

| Asset | Approximate dollar value |
|---|---|
| Employees and customer PII | $50,000,000 |
| Source code and software | $30,000,000 |
| Financial resources | $20,000,000 |
| Email server | $60,000,000 |
| Reputation | $70,000,000 |

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

| Asset | Potential vulnerabilities |
|---|---|
| Employees and customer PII | Unauthorized access |
| Source code and software | Bugs in source code and software |
| Financial resources | Unauthorized access |
| Email server | Administrative access to modify the mail server |
| Reputation | Disgruntled employee |

e) List of potential threats to Secure Systems that could exploit vulnerabilities of critical assets

| Asset | Potential threats |
|---|---|
| Employees and customer PII | Leaked PII data |
| | Ransomware |
| Source code and software | Remote code execution |
| | Disabling or crashing the system |
| Financial resources | Leaked confidential financial data |
| Email server | DOS threats |

| | |
|---|---|
| | Leaked confidential emails |
| Reputation | Leaking confidential company data |
| | Whistleblowers |

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

| **Missing control** | **Potential risks** |
|---|---|
| Static routes for sensitive data transfer | Leaked PII data |
| | Ransomware |
| Backdoor connections | Remote code execution |
| | Disabling or crashing the system |
| Hybrid technology firewall | Leaked confidential financial data |
| Application proxy firewall | DOS threats |
| | Leaked confidential emails |
| Secure router planes | Leaking confidential company data |
| | Whistleblowers |

g) 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

| **Potential vulnerabilities** | **Prevention controls** |
|---|---|
| Unauthorized access | Implementing strict access control mechanism to allow access to employees and customer PII |
| | Encrypting the data with the latest and great cryptographic algorithms |

| | |
|---|---|
| Bugs in source code and software | Static and dynamic code analysis before source code/software is deployed in productions |
| | Red teaming to identify vulnerabilities from an attacker perspective |
| Administrative access to modify the mail server | Hardening access to the mail server and implementing strict access control mechanisms |
| | Using SMIME for confidential emails |
| Disgruntled employee | Treating all employees with respect and dignity - important in work culture |

h) 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

| **Asset** | **Response controls** |
|---|---|
| Employees and customer PII | Store only data that is necessary |
| | Delete unnecessary data |
| Source code and software | Avoid storing source code in vulnerable systems |
| | Have a protected centralized repository for source code and software |
| | Training for developers on how to handle source code and software securely |
| Financial resources | Store only necessary data and delete the rest |
| | Education employees dealing with financial data about best practices and risks |
| Email server | No single point of failure |
| | Periodic maintenance of servers with latest updates |
| Reputation | Having a transparent and open culture |
| | Third-party and independent reviews to understand and address employee concerns |

8. Applicable Government Regulations and Industry Standards discussed in Class 12

**PCI-DSS**

One of the most important cybersecurity standards of our time considering the number of transactions that are being carried out with credit cards is the - PCI DSS (Payment Card Industry Data Security Standard)

Introduced in 2008, it is used by all major credit card issuers.

My previous organization had to be compliant with this standard as they accepted payments from credit cards. Some of the key factors that the organization worked on include - securing the network, protecting the data, and vulnerability management.

All the credit card and PII data was always encrypted according to the latest cryptographic standards. Testing the controls and encryption was done regularly with the help of red teams. Vulnerability management for zero days and patch updates was performed regularly.

**Sarbanes-Oxley Act**

It is US federal law according to which public companies are mandated to publishing accurate financial records. There are many provisions that are applicable to privately owned companies as well. This law was enacted in 2002 in response to major corporate and accounting scandals with companies like Enron and WorldCom.

Some of the key provisions in the law include:

Section 302 – All the financial disclosures have to be accurate. External auditors can also be used to remove any conflict of interest.

Section 303 – This section ensures that there is no improper influence on conducting the audits and the interests of shareholders, investors must be protected.

Section 401 – Periodic disclosure of off-balance items/ reports have to be done to show accurate status of finances in the organization.

Section 404 – This section requires management and external auditors to report on the adequacy of the company’s internal control on financial reporting.

9. Rank asset risks and vulnerability risks for Secure Systems across Access Control.

| Domain | Top 5 asset risks | Top 5 vulnerability risks |
|---|---|---|
| **Access Control** | Leaked PII data | Disabling or crashing the system |
| | Leaked confidential emails | Ransomware |
| | Leaked confidential company data | Source code bugs and vulnerabilites |
| | Social Engineering | Remote code execution |
| | Leaked source code | Sensitive information disclosure |
| **Network infrastructure** | Unauthorized access | Source code bugs and vulnerabilites |
| | DOS threat | Remote code execution |
| | Leaked PII data | Sensitive information disclosure |
| | Leaked confidential emails | Disabling or crashing the system |
| | Leaked confidential company data | Ransomware |
| **Network infrastructure management** | Leaked PII data | Remote code execution |
| | Leaked confidential emails | Sensitive information disclosure |
| | Leaked confidential company data | Disabling or crashing the system |
| | Unauthorized access | Ransomware |
| | DOS threat | Source code bugs and vulnerabilites |
| **Database** | Leaked confidential company data | Ransomware |
| | Unauthorized access | Source code bugs and vulnerabilites |
| | DOS threat | Remote code execution |
| | Leaked PII data | Sensitive information disclosure |
| | Leaked confidential emails | Disabling or crashing the system |
| **Applications** | Unauthorized access | Remote code execution |
| | DOS threat | Sensitive information disclosure |
| | Leaked PII data | Disabling or crashing the system |

| | | |
|---|---|---|
| | Leaked confidential emails | Ransomware |
| | Leaked confidential company data | Source code bugs and vulnerabilites |
| **Wireless** | Leaked PII data | Ransomware |
| | Leaked confidential emails | Source code bugs and vulnerabilites |
| | Leaked confidential company data | Remote code execution |
| | Unauthorized access | Sensitive information disclosure |
| | DOS threat | Disabling or crashing the system |

Across all categories

| **Top 5 asset risks** |
|---|
| Leaked PII data |
| Leaked confidential emails |
| Leaked confidential company data |
| Social Engineering |
| Leaked source code |

| **Top 5 vulnerability risks** |
|---|
| Disabling or crashing the system |
| Ransomware |
| Source code bugs and vulnerabilites |
| Remote code execution |
| Sensitive information disclosure |

10. Cybersecurity Workforce Risk Management Implementation

a. List of Cybersecurity Specialty Areas that exist in Secure Systems.

| **NICE specialty Area** |
|---|
| Risk Management (RSK) |
| Systems Development (SYS) |
| Executive Cyber Leadership (EXL) |
| Cybersecurity Defense Infrastructure Support (INF) |
| All-Source Analysis (ASA) |
| Cyber Operations (OPS) |
| Digital Forensics (FOR) |

b. List of Cybersecurity Work Roles that exist in Secure Systems

| **Work role** |
|---|
| Authorizing Official/Designating Representative |
| Security Control Assessor |
| Information Systems Security Developer |
| Systems Developer |
| Executive Cyber Leadership |
| Cyber Defense Infrastructure Support Specialist |
| All-Source Analyst |
| Mission Assessment Specialist |
| Cyber Operator |
| Law Enforcement /Counterintelligence Forensics Analyst |
| Cyber Defense Forensics Analyst |

c. List of Cybersecurity Tasks that exist in Secure Systems

| **Task ID** | **Task** |
|---|---|
| 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). |

| | |
|---|---|
| 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. |
| T0255 | Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. |
| T0264 | Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. |
| T0265 | 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. |
| T0268 | Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. |
| T0272 | Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. |
| T0275 | Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). |
| T0277 | Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. |
| T0309 | Assess the effectiveness of security controls. |
| T0344 | Assess all the configuration management (change configuration/release management) processes. |
| 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. |
| T0018 | Assess the effectiveness of cybersecurity measures utilized by system(s). |
| T0019 | Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile. |
| T0272 | Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. |
| T0304 | Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment. |
| T0326 | Employ configuration management processes. |

| | |
|---|---|
| T0359 | Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. |
| T0446 | Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation. |
| T0449 | Design to security requirements to ensure requirements are met for all systems and/or applications. |
| T0466 | Develop mitigation strategies to address cost, schedule, performance, and security risks. |
| T0509 | Perform an information security risk assessment. |
| T0518 | Perform security reviews and identify security gaps in architecture. |
| T0527 | Provide input to implementation plans and standard operating procedures as they relate to information systems security. |
| T0541 | Trace system requirements to design components and perform gap analysis. |
| T0544 | Verify stability, interoperability, portability, and/or scalability of system architecture. |
| 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). |
| T0109 | 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. |
| 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. |
| T0181 | Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. |
| T0201 | Provide guidelines for implementing developed systems to customers or installation teams. |
| 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). |
| T0228 | Store, retrieve, and manipulate data for analysis of system capabilities and requirements. |
| T0242 | Utilize models and simulations to analyze or predict system performance under different operating conditions. |
| T0304 | Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment. |
| T0326 | Employ configuration management processes. |
| T0350 | Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements. |

| | |
|---|---|
| T0358 | Design and develop system administration and management functionality for privileged access users. |
| T0359 | Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. |
| T0378 | Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle). |
| T0406 | Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary. |
| T0148 | Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. |
| T0151 | Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. |
| T0227 | Recommend policy and coordinate review and approval. |
| T0229 | Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. |
| T0229 | Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. |
| T0248 | Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. |
| T0254 | Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. |
| T0263 | Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. |
| T0264 | Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. |
| T0282 | Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate. |
| T0337 | Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. |
| T0356 | Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. |
| T0429 | Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. |
| T0445 | Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan. |
| T0509 | Perform an information security risk assessment. |
| T0763 | Conduct long-range, strategic planning efforts with internal and external partners in cyber 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. |

| | |
|---|---|
| T0180 | Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. |
| T0261 | Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources. |
| T0335 | Build, install, configure, and test dedicated cyber defense hardware. |
| T0348 | Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure. |
| T0420 | Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s). |
| T0438 | Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems). |
| T0483 | Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization). |
| 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. |
| T0687 | Identify threats to Blue Force vulnerabilities. |
| T0707 | Generate requests for information. |
| T0708 | Identify threat tactics, and methodologies. |
| T0710 | Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. |
| T0713 | Identify and submit intelligence requirements for the purposes of designating priority information requirements. |
| T0718 | Identify intelligence gaps and shortfalls. |
| T0748 | Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. |
| T0749 | Monitor and report on validated threat activities. |
| T0751 | Monitor open source websites for hostile content directed towards organizational or partner interests. |
| T0752 | Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements. |
| T0758 | Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). |
| T0761 | Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. |
| T0771 | Provide subject matter expertise to website characterizations. |
| T0782 | Provide analyses and support for effectiveness assessment. |
| T0593 | Brief threat and/or target current situations. |
| T0597 | Collaborate with intelligence analysts/targeting organizations involved in related areas. |

| | |
|---|---|
| T0611 | Conduct end-of-operations assessments. |
| T0615 | Conduct in-depth research and analysis. |
| T0617 | Conduct nodal analysis. |
| T0624 | Conduct target research and analysis. |
| T0660 | Develop information requirements necessary for answering priority information requests. |
| T0661 | Develop measures of effectiveness and measures of performance. |
| T0663 | Develop munitions effectiveness assessment or operational assessment materials. |
| T0678 | Engage customers to understand customers' intelligence needs and wants. |
| T0684 | Estimate operational effects generated through cyber activities. |
| T0685 | Evaluate threat decision-making processes. |
| T0686 | Identify threat vulnerabilities. |
| T0623 | Conduct survey of computer and digital networks. |
| T0643 | Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers). |
| T0644 | Detect exploits against targeted networks and hosts and react accordingly. |
| 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. |
| T0696 | Exploit network devices, security devices, and/or terminals or environments using various methods or tools. |
| T0697 | Facilitate access enabling by physical and/or wireless means. |
| T0724 | Identify potential points of strength and vulnerability within a network. |
| T0740 | Maintain situational awareness and functionality of organic operational infrastructure. |
| T0756 | Operate and maintain automated systems for gaining and maintaining access to target systems. |
| T0768 | Conduct cyber activities to degrade/remove information resident in computers and computer networks. |
| 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). |
| T0220 | Resolve conflicts in laws, regulations, policies, standards, or procedures. |
| T0308 | Analyze incident data for emerging trends. |
| T0398 | Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. |
| T0419 | Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. |
| T0401 | Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. |

| | |
|---|---|
| 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). |
| T0411 | Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. |
| T0425 | Analyze organizational cyber policy. |
| 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. |
| T0049 | Decrypt seized data using technical means. |
| T0075 | Provide technical summary of findings in accordance with established reporting procedures. |
| T0087 | Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence. |
| T0103 | Examine recovered data for information of relevance to the issue at hand. |
| T0113 | Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. |
| 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. |
| T0167 | Perform file signature analysis. |

d. Comparison of the NCWF recommended Cybersecurity Specialty Areas with Secure Systems’s existing Cybersecurity Specialty Areas

| **NICE Specialty Area** | **Status** |
|---|---|
| Securely Provision (SP) | Present |
| Risk Management (RSK) | Absent |
| Software Development (DEV) | Present |
| Systems Architecture (ARC) | Absent |
| Technology R&D (TRD) | Absent |
| Systems Requirements Planning (SRP) | Absent |
| Test and Evaluation (TST) | Absent |
| Systems Development (SYS) | Absent |
| Operate and Maintain (OM) | Absent |
| Data Administration (DTA) | Absent |
| Knowledge Management (KMG) | Present |
| Customer Service and Technical Support (STS) | Absent |
| Network Services (NET) | Absent |
| Systems Administration (ADM) | Absent |

| | |
|---|---|
| Systems Analysis (ANA) | Absent |
| Oversee and Govern (OV) | Present |
| Legal Advice and Advocacy (LGA) | Present |
| Training, Education, and Awareness (TEA) | Present |
| Cybersecurity Management (MGT) | Present |
| Strategic Planning and Policy (SPP) | Absent |
| Executive Cyber Leadership (EXL) | Present |
| Program/Project Management (PMA) and Acquisition | Present |
| Protect and Defend (PR) | Present |
| Cybersecurity Defense Analysis (CDA) | Absent |
| Cybersecurity Defense Infrastructure Support (INF) | Absent |
| Incident Response (CIR) | Absent |
| Vulnerability Assessment and Management (VAM) | Absent |
| Analyze (AN) | Absent |
| Threat Analysis (TWA) | Present |
| Exploitation Analysis (EXP) | Absent |
| All-Source Analysis (ASA) | Present |
| Targets (TGT) | Absent |
| Language Analysis (LNG) | Present |
| Collect and Operate (CO) | Absent |
| Collection Operations (CLO) | Present |
| Cyber Operational Planning (OPL) | Absent |
| Cyber Operations (OPS) | Absent |
| Investigate (IN) | Absent |
| Cyber Investigation (INV) | Absent |
| Digital Forensics (FOR) | Present |

e. Comparison of the NCWF recommended Cybersecurity Work Roles with Secure Systems's existing Cybersecurity Work Roles

| Work role | Status |
|---|---|
| Authorizing Official/Designating Representative | Absent |
| Security Control Assessor | Present |
| Information Systems Security Developer | Present |
| Systems Developer | Present |
| Executive Cyber Leadership | Absent |
| Cyber Defense Infrastructure Support Specialist | Present |
| All-Source Analyst | Present |
| Mission Assessment Specialist | Present |
| Cyber Operator | Absent |
| Law Enforcement /Counterintelligence Forensics Analyst | Absent |
| Cyber Defense Forensics Analyst | Present |

f. Comparison the NCWF recommended Cybersecurity Tasks with Secure Systems's existing Cybersecurity Tasks

| Task ID | Task Description | Status |
|---|---|---|
| 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. | Present |
| T0002 | Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program. | Present |
| T0003 | Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. | Absent |
| T0004 | Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| T0005 | Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture. | Present |
| T0006 | Advocate organization's official position in legal and legislative proceedings. | Absent |

| | | |
|---|---|---|
| T0007 | Analyze and define data requirements and specifications. | Present |
| T0008 | Analyze and plan for anticipated changes in data capacity requirements. | Present |
| T0009 | Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application. | Absent |
| T0010 | Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. | Absent |
| T0011 | Analyze user needs and software requirements to determine feasibility of design within time and cost constraints. | Absent |
| T0012 | Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. | Present |
| T0013 | Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. | Absent |
| T0014 | Apply secure code documentation. | Present |
| T0015 | Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications. | Absent |
| T0016 | Apply security policies to meet security objectives of the system. | Absent |
| T0017 | Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | Present |
| T0018 | Assess the effectiveness of cybersecurity measures utilized by system(s). | Present |
| T0019 | Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile. | Present |
| T0020 | Develop content for cyber defense tools. | Present |
| T0021 | Build, test, and modify product prototypes using working models or theoretical models. | Absent |
| T0022 | 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 |
| T0023 | Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources. | Present |

| | | |
|---|---|---|
| T0024 | Collect and maintain data needed to meet system cybersecurity reporting. | Absent |
| T0025 | Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Present |
| T0026 | Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program. | Present |
| T0027 | Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. | Present |
| T0028 | Conduct and/or support authorized penetration testing on enterprise network assets. | Present |
| T0029 | Conduct functional and connectivity testing to ensure continuing operability. | Absent |
| T0030 | Conduct interactive training exercises to create an effective learning environment. | Absent |
| T0031 | Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects. | Present |
| T0032 | Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII). | Absent |
| T0033 | Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications. | Absent |
| 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. | Present |
| T0035 | Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling). | Present |
| T0036 | Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. | Present |
| T0037 | Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users. | Absent |
| T0038 | Develop threat model based on customer interviews and requirements. | Present |

| | | |
|---|---|---|
| T0039 | Consult with customers to evaluate functional requirements. | Present |
| T0040 | Consult with engineering staff to evaluate interface between hardware and software. | Present |
| T0041 | Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. | Present |
| 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. | Present |
| T0043 | Coordinate with enterprise-wide cyber defense staff to validate network alerts. | Absent |
| T0044 | Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. | Present |
| T0045 | Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions. | Present |
| T0046 | Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced. | Present |
| T0047 | Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. | Present |
| 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. | Present |
| T0049 | Decrypt seized data using technical means. | Present |
| T0050 | Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. | Present |
| 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 | Absent |

| | | |
|---|---|---|
| | supportability requirements for system recover/restoration. | |
| T0052 | Define project scope and objectives based on customer requirements. | Absent |
| T0053 | Design and develop cybersecurity or cybersecurity-enabled products. | Absent |
| T0054 | Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs. | Absent |
| T0055 | Design hardware, operating systems, and software applications to adequately address cybersecurity requirements. | Present |
| 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. | Present |
| T0057 | Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design. | Present |
| T0058 | Determine level of assurance of developed capabilities based on test results. | Absent |
| T0059 | Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. | Present |
| T0060 | Develop an understanding of the needs and requirements of information end-users. | Absent |
| T0061 | Develop and direct system testing and validation procedures and documentation. | Absent |
| T0062 | Develop and document requirements, capabilities, and constraints for design procedures and processes. | Present |
| T0063 | Develop and document systems administration standard operating procedures. | Absent |
| T0064 | Review and validate data mining and data warehousing programs, processes, and requirements. | Present |

| | | |
|---|---|---|
| T0065 | Develop and implement network backup and recovery procedures. | Present |
| T0066 | Develop and maintain strategic plans. | Present |
| T0067 | Develop architectures or system components consistent with technical specifications. | Absent |
| T0068 | Develop data standards, policies, and procedures. | Present |
| T0069 | Develop detailed security design documentation for component and interface specifications to support system design and development. | Present |
| T0070 | Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | Present |
| 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). | Absent |
| T0072 | Develop methods to monitor and measure risk, compliance, and assurance efforts. | Absent |
| T0073 | Develop new or identify existing awareness and training materials that are appropriate for intended audiences. | Absent |
| T0074 | Develop policy, programs, and guidelines for implementation. | Present |
| T0075 | Provide technical summary of findings in accordance with established reporting procedures. | Absent |
| T0076 | Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed. | Absent |
| T0077 | Develop secure code and error handling. | Absent |
| T0078 | Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications. | Absent |
| T0079 | Develop specifications to ensure that risk, compliance, and assurance efforts conform with security, resilience, and dependability requirements at the software application, system, and network environment level. | Present |
| T0080 | Develop test plans to address specifications and requirements. | Present |
| T0081 | Diagnose network connectivity problem. | Present |

| | | |
|---|---|---|
| T0082 | Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. | Absent |
| T0083 | Draft statements of preliminary or residual security risks for system operation. | Absent |
| T0084 | Employ secure configuration management processes. | Absent |
| T0085 | Ensure all systems security operations and maintenance activities are properly documented and updated as necessary. | Absent |
| 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. | Present |
| T0087 | Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence. | Present |
| T0088 | Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. | Present |
| T0089 | Ensure that security improvement actions are evaluated, validated, and implemented as required. | Absent |
| T0090 | Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. | Present |
| T0091 | Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment. | Present |
| T0092 | Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s). | Present |
| T0093 | Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture. | Absent |
| T0094 | Establish and maintain communication channels with stakeholders. | Absent |
| T0095 | Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy. | Absent |

| | | |
|---|---|---|
| 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). | Absent |
| T0097 | Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed. | Present |
| T0098 | Evaluate contracts to ensure compliance with funding, legal, and program requirements. | Absent |
| T0099 | Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Present |
| T0100 | Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. | Present |
| T0101 | Evaluate the effectiveness and comprehensiveness of existing training programs. | Present |
| T0102 | Evaluate the effectiveness of laws, regulations, policies, standards, or procedures. | Absent |
| T0103 | Examine recovered data for information of relevance to the issue at hand. | Absent |
| T0104 | Fuse computer network attack analyses with criminal and counterintelligence investigations and operations. | Absent |
| T0105 | Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements. | Absent |
| T0106 | Identify alternative information security strategies to address organizational security objective. | Absent |
| 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). | Absent |
| T0108 | Identify and prioritize critical business functions in collaboration with organizational stakeholders. | Present |
| T0109 | Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability. | Absent |

| | | |
|---|---|---|
| T0110 | Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action. | Absent |
| T0111 | Identify basic common coding flaws at a high level. | Present |
| T0112 | Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations. | Absent |
| T0113 | Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. | Present |
| T0114 | Identify elements of proof of the crime. | Present |
| T0115 | Identify information technology (IT) security program implications of new technologies or technology upgrades. | Present |
| T0116 | Identify organizational policy stakeholders. | Present |
| T0117 | Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. | Absent |
| T0118 | Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life. | Absent |
| 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. | Absent |
| T0120 | Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations. | Absent |
| T0121 | Implement new system design procedures, test procedures, and quality standards. | Absent |
| T0122 | Implement security designs for new or existing system(s). | Present |
| T0123 | Implement specific cybersecurity countermeasures for systems and/or applications. | Absent |
| T0124 | Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts). | Present |
| T0125 | Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Absent |

| | | |
|---|---|---|
| T0126 | Install or replace network hubs, routers, and switches. | Present |
| T0127 | Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements. | Present |
| T0128 | Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. | Absent |
| T0129 | Integrate new systems into existing network architecture. | Absent |
| T0130 | Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information. | Absent |
| T0131 | Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. | Absent |
| T0132 | Interpret and/or approve security requirements relative to the capabilities of new information technologies. | Absent |
| T0133 | Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program. | Present |
| T0134 | Lead and align information technology (IT) security priorities with the security strategy. | Absent |
| T0135 | Lead and oversee information security budget, staffing, and contracting. | Present |
| T0136 | Maintain baseline system security according to organizational policies. | Absent |
| T0137 | Maintain database management systems software. | Present |
| T0138 | Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. | Absent |
| T0139 | Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing. | Absent |
| T0140 | Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required. | Absent |

| | | |
|---|---|---|
| T0141 | Maintain information systems assurance and accreditation materials. | Present |
| T0142 | Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. | Present |
| T0143 | Make recommendations based on test results. | Absent |
| T0144 | Manage accounts, network rights, and access to systems and equipment. | Absent |
| T0145 | Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). | Absent |
| T0146 | Manage the compilation, cataloging, caching, distribution, and retrieval of data. | Present |
| T0147 | Manage the monitoring of information security data sources to maintain organizational situational awareness. | Present |
| T0148 | Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. | Present |
| T0149 | Manage threat or target analysis of cyber defense information and production of threat information within the enterprise. | Absent |
| T0150 | Monitor and evaluate a system's compliance with information technology (IT) security, resilience, and dependability requirements. | Absent |
| T0151 | Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. | Absent |
| T0152 | Monitor and maintain databases to ensure optimal performance. | Absent |
| T0153 | Monitor network capacity and performance. | Absent |
| T0154 | Monitor and report the usage of knowledge management assets and resources. | Absent |
| T0155 | 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 |
| T0156 | Oversee and make recommendations regarding configuration management. | Absent |
| T0157 | Oversee the information security training and awareness program. | Present |

| | | |
|---|---|---|
| T0158 | Participate in an information security risk assessment during the Security Assessment and Authorization process. | Absent |
| T0159 | Participate in the development or modification of the computer environment cybersecurity program plans and requirements. | Absent |
| T0160 | Patch network vulnerabilities to ensure that information is safeguarded against outside parties. | Present |
| T0161 | 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 |
| T0162 | Perform backup and recovery of databases to ensure data integrity. | Present |
| 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. | Present |
| T0164 | Perform cyber defense trend analysis and reporting. | Absent |
| 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. | Present |
| 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. | Present |
| T0167 | Perform file signature analysis. | Present |
| T0168 | Perform hash comparison against established database. | Absent |
| T0169 | Perform cybersecurity testing of developed applications and/or systems. | Present |
| T0170 | Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. | Absent |
| T0171 | Perform integrated quality assurance testing for security functionality and resiliency attack. | Absent |
| T0172 | Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView). | Present |
| T0173 | Perform timeline analysis. | Absent |

| | | |
|---|---|---|
| T0174 | Perform needs analysis to determine opportunities for new and improved business process solutions. | Absent |
| T0175 | Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). | Present |
| T0176 | Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities. | Absent |
| T0177 | Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. | Present |
| T0178 | Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. | Present |
| T0179 | Perform static media analysis. | Present |
| T0180 | Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. | Present |
| T0181 | Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Present |
| T0182 | Perform tier 1, 2, and 3 malware analysis. | Present |
| T0183 | Perform validation steps, comparing actual results with expected results and analyze the differences to identify impact and risks. | Absent |
| T0184 | Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks. | Absent |
| T0185 | Plan and manage the delivery of knowledge management projects. | Present |
| T0186 | Plan, execute, and verify data redundancy and system recovery procedures. | Present |
| T0187 | Plan and recommend modifications or adjustments based on exercise results or system environment. | Absent |
| T0188 | Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. | Present |
| T0189 | Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and | Absent |

| | | |
|---|---|---|
| | convert them into a series of instructions coded in a computer language. | |
| T0190 | Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures). | Absent |
| T0191 | Prepare use cases to justify the need for specific information technology (IT) solutions. | Absent |
| T0192 | Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations. | Absent |
| T0193 | Process crime scenes. | Present |
| T0194 | Properly document all systems security implementation, operations, and maintenance activities and update as necessary. | Absent |
| T0195 | Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | Absent |
| T0196 | Provide advice on project costs, design concepts, or design changes. | Absent |
| T0197 | Provide an accurate technical evaluation of the software application, system, or network, documenting the security posture, capabilities, and vulnerabilities against relevant cybersecurity compliances. | Present |
| T0198 | Provide daily summary reports of network events and activity relevant to cyber defense practices. | Present |
| T0199 | Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | Present |
| T0200 | Provide feedback on network requirements, including network architecture and infrastructure. | Absent |
| T0201 | Provide guidelines for implementing developed systems to customers or installation teams. | Present |
| T0202 | Provide cybersecurity guidance to leadership. | Present |
| T0203 | Provide input on security requirements to be included in statements of work and other appropriate procurement documents. | Absent |
| T0204 | Provide input to implementation plans and standard operating procedures. | Absent |

| | | |
|---|---|---|
| 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). | Absent |
| T0206 | Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities. | Present |
| T0207 | Provide ongoing optimization and problem-solving support. | Present |
| T0208 | Provide recommendations for possible improvements and upgrades. | Present |
| T0209 | Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information. | Absent |
| T0210 | Provide recommendations on new database technologies and architectures. | Present |
| T0211 | Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents. | Present |
| T0212 | Provide technical assistance on digital evidence matters to appropriate personnel. | Present |
| T0213 | Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters. | Absent |
| T0214 | Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. | Present |
| T0215 | Recognize a possible security violation and take appropriate action to report the incident, as required. | Present |
| T0216 | Recognize and accurately report forensic artifacts indicative of a particular operating system. | Present |
| T0217 | Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. | Absent |
| T0218 | Recommend new or revised security, resilience, and dependability measures based on the results of reviews. | Absent |

| | | |
|---|---|---|
| T0219 | Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements. | Absent |
| T0220 | Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| T0221 | Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. | Absent |
| T0222 | Review existing and proposed policies with stakeholders. | Absent |
| T0223 | Review or conduct audits of information technology (IT) programs and projects. | Absent |
| T0224 | Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions). | Present |
| T0225 | Secure the electronic device or information source. | Absent |
| T0226 | Serve on agency and interagency policy boards. | Absent |
| T0227 | Recommend policy and coordinate review and approval. | Present |
| T0228 | Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Absent |
| T0229 | Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Present |
| T0230 | Support the design and execution of exercise scenarios. | Absent |
| T0231 | Provide support to security/certification test and evaluation activities. | Present |
| T0232 | Test and maintain network infrastructure including software and hardware devices. | Absent |
| T0233 | Track and document cyber defense incidents from initial detection through final resolution. | Absent |
| T0234 | Track audit findings and recommendations to ensure that appropriate mitigation actions are taken. | Absent |
| T0235 | Translate functional requirements into technical solutions. | Present |
| T0236 | Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria. | Absent |

| | | |
|---|---|---|
| T0237 | Troubleshoot system hardware and software. | Present |
| T0238 | Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost). | Present |
| T0239 | Use federal and organization-specific published documents to manage operations of their computing environment system(s). | Present |
| T0240 | Capture and analyze network traffic associated with malicious activities using network monitoring tools. | Present |
| T0241 | Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. | Absent |
| T0242 | Utilize models and simulations to analyze or predict system performance under different operating conditions. | Present |
| T0243 | Verify and update security documentation reflecting the application/system security design features. | Present |
| T0244 | Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. | Present |
| T0245 | Verify that the software application/network/system accreditation and assurance documentation is current. | Absent |
| T0246 | Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. | Absent |
| T0247 | Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. | Absent |
| T0248 | Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. | Absent |
| T0249 | Research current technology to understand capabilities of required system or network. | Absent |
| T0250 | Identify cyber capabilities strategies for custom hardware and software development based on mission requirements. | Present |
| T0251 | Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers). | Present |

| | | |
|---|---|---|
| T0252 | Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews). | Absent |
| T0253 | Conduct cursory binary analysis. | Present |
| T0254 | Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. | Absent |
| T0255 | Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. | Present |
| T0256 | Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Present |
| T0257 | Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated. | Present |
| 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. | Present |
| T0259 | Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity. | Absent |
| T0260 | Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. | Absent |
| T0261 | Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources. | Absent |
| T0262 | Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness). | Present |
| T0263 | Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. | Absent |
| T0264 | Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. | Absent |

| | | |
|---|---|---|
| T0265 | Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals. | Absent |
| T0266 | Perform penetration testing as required for new or updated applications. | Absent |
| T0267 | Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements. | Present |
| T0268 | Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. | Present |
| T0269 | Design and develop key management functions (as related to cybersecurity). | Present |
| T0270 | Analyze user needs and requirements to plan and conduct system security development. | Absent |
| T0271 | Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information). | Present |
| T0272 | Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. | Present |
| T0273 | Develop and document supply chain risks for critical system elements, as appropriate. | Absent |
| T0274 | Create auditable evidence of security measures. | Present |
| T0275 | Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). | Absent |
| T0276 | Participate in the acquisition process as necessary, following appropriate supply chain risk management practices. | Present |
| T0277 | Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |

| | | |
|---|---|---|
| T0278 | 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 |
| T0279 | Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. | Absent |
| T0280 | Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance. | Absent |
| T0281 | Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary. | Absent |
| T0282 | Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate. | Absent |
| T0283 | Collaborate with stakeholders to identify and/or develop appropriate solutions technology. | Absent |
| T0284 | Design and develop new tools/technologies as related to cybersecurity. | Present |
| T0285 | Perform virus scanning on digital media. | Present |
| T0286 | Perform file system forensic analysis. | Present |
| T0287 | Perform static analysis to mount an "image" of a drive (without necessarily having the original drive). | Present |
| T0288 | Perform static malware analysis. | Present |
| T0289 | Utilize deployable forensics toolkit to support operations as necessary. | Present |
| T0290 | Determine tactics, techniques, and procedures (TTPs) for intrusion sets. | Present |
| T0291 | Examine network topologies to understand data flows through the network. | Present |
| T0292 | Recommend computing environment vulnerability corrections. | Present |
| T0293 | Identify and analyze anomalies in network traffic using metadata. | Absent |
| T0294 | Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). | Absent |
| T0295 | Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. | Present |
| T0296 | Isolate and remove malware. | Absent |
| T0297 | Identify applications and operating systems of a network device based on network traffic. | Present |

| | | |
|---|---|---|
| T0298 | Reconstruct a malicious attack or activity based off network traffic. | Absent |
| T0299 | Identify network mapping and operating system (OS) fingerprinting activities. | Absent |
| T0300 | Develop and document User Experience (UX) requirements including information architecture and user interface requirements. | Present |
| T0301 | Develop and implement cybersecurity independent audit processes for application software/networks/systems and oversee ongoing independent audits to ensure that operational and Research and Design (R&D) processes and procedures are in compliance with organizational and mandatory cybersecurity requirements and accurately followed by Systems Administrators and other cybersecurity staff when performing their day-to-day activities. | Absent |
| T0302 | Develop contract language to ensure supply chain, system, network, and operational security are met. | Present |
| T0303 | Identify and leverage the enterprise-wide version control system while designing and developing secure applications. | Absent |
| T0304 | Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment. | Absent |
| T0305 | Performs configuration management, problem management, capacity management, and financial management for databases and data management systems. | Absent |
| T0306 | Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems. | Present |
| T0307 | Analyze candidate architectures, allocate security services, and select security mechanisms. | Absent |
| T0308 | Analyze incident data for emerging trends. | Present |
| T0309 | Assess the effectiveness of security controls. | Present |
| T0310 | Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave. | Absent |
| T0311 | Consult with customers about software system design and maintenance. | Present |

| | | |
|---|---|---|
| T0312 | Coordinate with intelligence analysts to correlate threat assessment data. | Present |
| T0313 | Design and document quality standards. | Absent |
| T0314 | Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | Absent |
| T0315 | Develop and deliver technical training to educate others or meet customer needs. | Absent |
| T0316 | Develop or assist in the development of computer based training modules or classes. | Present |
| T0317 | Develop or assist in the development of course assignments. | Absent |
| T0318 | Develop or assist in the development of course evaluations. | Absent |
| T0319 | Develop or assist in the development of grading and proficiency standards. | Absent |
| T0320 | Assist in the development of individual/collective development, training, and/or remediation plans. | Present |
| T0321 | Develop or assist in the development of learning objectives and goals. | Absent |
| T0322 | Develop or assist in the development of on-the-job training materials or programs. | Present |
| T0323 | Develop or assist in the development of written tests for measuring and assessing learner proficiency. | Present |
| T0324 | Direct software programming and development of documentation. | Absent |
| T0325 | Document a system's purpose and preliminary system security concept of operations. | Present |
| T0326 | Employ configuration management processes. | Absent |
| T0327 | Evaluate network infrastructure vulnerabilities to enhance capabilities being developed. | Present |
| 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. | Present |
| T0329 | Follow software and systems engineering life cycle standards and processes. | Present |
| T0330 | Maintain assured message delivery systems. | Absent |
| T0331 | Maintain incident tracking and solution database. | Present |

| | | |
|---|---|---|
| T0332 | 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 |
| T0333 | Perform cyber defense trend analysis and reporting. | Absent |
| T0334 | Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware). | Absent |
| T0335 | Build, install, configure, and test dedicated cyber defense hardware. | Absent |
| T0336 | **WITHDRAWN:** Integrated with T0228 | Present |
| T0337 | Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Present |
| T0338 | Write detailed functional specifications that document the architecture development process. | Absent |
| T0339 | Lead efforts to promote the organization's use of knowledge management and information sharing. | Absent |
| T0340 | Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully. | Absent |
| T0341 | Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. | Absent |
| T0342 | Analyze data sources to provide actionable recommendations. | Present |
| T0343 | Analyze the crisis to ensure public, personal, and resource protection. | Present |
| T0344 | Assess all the configuration management (change configuration/release management) processes. | Present |
| T0345 | Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction. | Absent |
| T0346 | Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation. | Present |
| T0347 | Assess the validity of source data and subsequent findings. | Present |

| | | |
|---|---|---|
| T0348 | Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure. | Absent |
| T0349 | Collect metrics and trending data. | Absent |
| T0350 | Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements. | Absent |
| T0351 | Conduct hypothesis testing using statistical processes. | Present |
| T0352 | Conduct learning needs assessments and identify requirements. | Present |
| T0353 | Confer with systems analysts, engineers, programmers, and others to design application. | Present |
| T0354 | Coordinate and manage the overall service provided to a customer end-to-end. | Absent |
| T0355 | Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards. | Present |
| T0356 | Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. | Present |
| T0357 | Create interactive learning exercises to create an effective learning environment. | Present |
| T0358 | Design and develop system administration and management functionality for privileged access users. | Present |
| T0359 | Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. | Present |
| T0360 | Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks. | Present |
| T0361 | Develop and facilitate data-gathering methods. | Present |
| T0362 | Develop and implement standardized position descriptions based on established cyber work roles. | Absent |
| T0363 | Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies. | Present |
| T0364 | Develop cyber career field classification structure to include establishing career field entry requirements | Present |

| | | |
|---|---|---|
| | and other nomenclature such as codes and identifiers. | |
| T0365 | Develop or assist in the development of training policies and protocols for cyber training. | Present |
| T0366 | Develop strategic insights from large data sets. | Absent |
| T0367 | Develop the goals and objectives for cyber curriculum. | Absent |
| T0368 | Ensure that cyber career fields are managed in accordance with organizational HR policies and directives. | Absent |
| T0369 | Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. | Present |
| T0370 | Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service. | Absent |
| T0371 | Establish acceptable limits for the software application, network, or system. | Absent |
| T0372 | Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel. | Absent |
| T0373 | Establish and oversee waiver processes for cyber career field entry and training qualification requirements. | Absent |
| T0374 | Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields. | Present |
| T0375 | Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements. | Absent |
| T0376 | Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements. | Absent |
| T0377 | Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Present |

| | | |
|---|---|---|
| T0378 | Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle). | Present |
| T0379 | Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). | Absent |
| 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. | Present |
| T0381 | Present technical information to technical and nontechnical audiences. | Absent |
| T0382 | Present data in creative formats. | Present |
| T0383 | Program custom algorithms. | Absent |
| T0384 | 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 |
| T0385 | Provide actionable recommendations to critical stakeholders based on data analysis and findings. | Absent |
| T0386 | Provide criminal investigative support to trial counsel during the judicial process. | Absent |
| T0387 | Review and apply cyber career field qualification standards. | Present |
| T0388 | Review and apply organizational policies related to or influencing the cyber workforce. | Present |
| T0389 | Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. | Absent |
| T0390 | Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. | Absent |
| T0391 | Support integration of qualified cyber workforce personnel into information systems life cycle development processes. | Present |
| T0392 | Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method. | Present |
| T0393 | Validate specifications and requirements for testability. | Absent |

| | | |
|---|---|---|
| T0394 | Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives. | Present |
| T0395 | Write and publish after action reviews. | Present |
| T0396 | Process image with appropriate tools depending on analyst's goals. | Present |
| T0397 | Perform Windows registry analysis. | Absent |
| T0398 | Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. | Present |
| T0399 | Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired. | Absent |
| T0400 | Correlate incident data and perform cyber defense reporting. | Absent |
| T0401 | Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. | Absent |
| T0402 | Effectively allocate storage capacity in the design of data management systems. | Absent |
| 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). | Present |
| T0404 | Utilize different programming languages to write code, open files, read files, and write output to different files. | Present |
| T0405 | 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 |
| T0406 | Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary. | Present |
| T0407 | Participate in the acquisition process as necessary. | Present |
| T0408 | Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. | Absent |

| | | |
|---|---|---|
| T0409 | Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases. | Present |
| T0410 | Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities. | Absent |
| T0411 | Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. | Present |
| T0412 | Conduct import/export reviews for acquiring systems and software. | Present |
| T0413 | Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce. | Absent |
| T0414 | Develop supply chain, system, network, performance, and cybersecurity requirements. | Present |
| T0415 | Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Present |
| T0416 | Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | Present |
| T0417 | Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate. | Present |
| T0418 | Install, update, and troubleshoot systems/servers. | Absent |
| T0419 | Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. | Absent |
| T0420 | Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s). | Present |
| T0421 | Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files). | Present |
| T0422 | Implement data management standards, requirements, and specifications. | Present |
| T0423 | Analyze computer-generated threats for counter intelligence or criminal activity. | Absent |

| | | |
|---|---|---|
| T0424 | Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application. | Absent |
| T0425 | Analyze organizational cyber policy. | Absent |
| T0426 | Analyze the results of software, hardware, or interoperability testing. | Present |
| T0427 | Analyze user needs and requirements to plan architecture. | Present |
| T0428 | Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates. | Present |
| T0429 | Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. | Absent |
| T0430 | Gather and preserve evidence used on the prosecution of computer crimes. | Present |
| T0431 | Check system hardware availability, functionality, integrity, and efficiency. | Absent |
| T0432 | Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. | Absent |
| T0433 | Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes. | Absent |
| T0434 | Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance. | Present |
| T0435 | Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing. | Absent |
| T0436 | Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct. | Present |
| T0437 | Correlate training and learning to business or mission requirements. | Absent |
| T0438 | Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems). | Absent |

| | | |
|---|---|---|
| T0439 | Detect and analyze encrypted data, stenography, alternate data streams and other forms of concealed data. | Present |
| T0440 | Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. | Absent |
| T0441 | Define and integrate current and future mission environments. | Absent |
| T0442 | Create training courses tailored to the audience and physical environment. | Absent |
| T0443 | Deliver training courses tailored to the audience and physical/virtual environments. | Present |
| T0444 | Apply concepts, procedures, software, equipment, and/or technology applications to students. | Present |
| T0445 | Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization's strategic plan. | Present |
| T0446 | Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation. | Absent |
| T0447 | Design hardware, operating systems, and software applications to adequately address requirements. | Present |
| T0448 | Develop enterprise architecture or system components required to meet user needs. | Present |
| T0449 | Design to security requirements to ensure requirements are met for all systems and/or applications. | Present |
| T0450 | Design training curriculum and course content based on requirements. | Absent |
| T0451 | Participate in development of training curriculum and course content. | Absent |
| T0452 | Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization's intellectual capital. | Absent |
| T0453 | Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes. | Present |
| T0454 | Define baseline security requirements in accordance with applicable guidelines. | Absent |
| T0455 | Develop software system testing and validation procedures, programming, and documentation. | Present |

| | | |
|---|---|---|
| T0456 | Develop secure software testing and validation procedures. | Absent |
| T0457 | Develop system testing and validation procedures, programming, and documentation. | Absent |
| T0458 | Comply with organization systems administration standard operating procedures. | Present |
| T0459 | Implement data mining and data warehousing applications. | Present |
| T0460 | Develop and implement data mining and data warehousing programs. | Absent |
| T0461 | Implement and enforce local network usage policies and procedures. | Present |
| T0462 | Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements. | Absent |
| T0463 | Develop cost estimates for new or modified system(s). | Present |
| T0464 | Develop detailed design documentation for component and interface specifications to support system design and development. | Absent |
| T0465 | Develop guidelines for implementation. | Present |
| T0466 | Develop mitigation strategies to address cost, schedule, performance, and security risks. | Present |
| T0467 | Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness. | Absent |
| T0468 | Diagnose and resolve customer reported system incidents, problems, and events. | Present |
| T0469 | Analyze and report organizational security posture trends. | Absent |
| T0470 | Analyze and report system security posture trends. | Absent |
| T0471 | Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking). | Present |
| T0472 | Draft, staff, and publish cyber policy. | Present |
| T0473 | Document and update as necessary all definition and architecture activities. | Present |
| T0474 | Provide legal analysis and decisions to inspectors general, privacy officers, oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements. | Absent |
| T0475 | Assess adequate access controls based on principles of least privilege and need-to-know. | Absent |

| | | |
|---|---|---|
| T0476 | Evaluate the impact of changes to laws, regulations, policies, standards, or procedures. | Absent |
| T0477 | Ensure the execution of disaster recovery and continuity of operations. | Absent |
| T0478 | Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. | Absent |
| T0479 | Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property. | Absent |
| T0480 | Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements. | Present |
| T0481 | Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training). | Absent |
| T0482 | Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience. | Absent |
| T0483 | Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization). | Present |
| T0484 | Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. | Absent |
| T0485 | Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed. | Present |
| 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. | Present |
| T0487 | Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures. | Absent |
| T0488 | Implement designs for new or existing system(s). | Present |
| T0489 | Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | Present |

| | | |
|---|---|---|
| T0490 | Install and configure database management systems and software. | Present |
| T0491 | Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards. | Present |
| T0492 | Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment. | Present |
| T0493 | Lead and oversee budget, staffing, and contracting. | Present |
| T0494 | Administer accounts, network rights, and access to systems and equipment. | Absent |
| T0495 | Manage Accreditation Packages (e.g., ISO/IEC 15026-2). | Absent |
| T0496 | Perform asset management/inventory of information technology (IT) resources. | Present |
| T0497 | Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements. | Absent |
| T0498 | Manage system/server resources including performance, capacity, availability, serviceability, and recoverability. | Absent |
| T0499 | Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative. | Absent |
| T0500 | Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance. | Present |
| T0501 | Monitor and maintain system/server configuration. | Present |
| T0502 | Monitor and report client-level computer system performance. | Present |
| T0503 | Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. | Present |
| T0504 | Assess and monitor cybersecurity related to system implementation and testing practices. | Absent |
| T0505 | Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. | Present |
| T0506 | Seek consensus on proposed policy changes from stakeholders. | Present |

| | | |
|---|---|---|
| T0507 | Oversee installation, implementation, configuration, and support of system components. | Present |
| T0508 | Verify minimum security requirements are in place for all applications. | Present |
| T0509 | Perform an information security risk assessment. | Absent |
| T0510 | Coordinate incident response functions. | Present |
| T0511 | Perform developmental testing on systems under development. | Present |
| T0512 | Perform interoperability testing on systems exchanging electronic information with other systems. | Present |
| T0513 | Perform operational testing. | Present |
| T0514 | Diagnose faulty system/server hardware. | Absent |
| T0515 | Perform repairs on faulty system/server hardware. | Absent |
| T0516 | Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities. | Present |
| T0517 | Integrate results regarding the identification of gaps in security architecture. | Present |
| T0518 | Perform security reviews and identify security gaps in architecture. | Present |
| T0519 | Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment. | Absent |
| T0520 | Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses). | Absent |
| T0521 | Plan implementation strategy to ensure that enterprise components can be integrated and aligned. | Present |
| T0522 | Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery). | Absent |
| T0523 | Prepare reports to document the investigation following legal standards and requirements. | Present |
| T0524 | Promote knowledge sharing between information owners/users through an organization’s operational processes and systems. | Present |
| T0525 | Provide enterprise cybersecurity and supply chain risk management guidance. | Present |

| | | |
|---|---|---|
| T0526 | Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. | Absent |
| T0527 | Provide input to implementation plans and standard operating procedures as they relate to information systems security. | Absent |
| T0528 | Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials | Present |
| T0529 | Provide policy guidance to cyber management, staff, and users. | Absent |
| T0530 | Develop a trend analysis and impact report. | Present |
| T0531 | Troubleshoot hardware/software interface and interoperability problems. | Present |
| T0532 | Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information. | Present |
| T0533 | Review, conduct, or participate in audits of cyber programs and projects. | Absent |
| T0534 | Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions). | Absent |
| T0535 | Recommend revisions to curriculum and course content based on feedback from previous training sessions. | Present |
| T0536 | Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). | Absent |
| T0537 | Support the CIO in the formulation of cyber-related policies. | Present |
| T0538 | Provide support to test and evaluation activities. | Absent |
| T0539 | Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements. | Present |
| T0540 | Record and manage test data. | Present |
| T0541 | Trace system requirements to design components and perform gap analysis. | Present |
| T0542 | Translate proposed capabilities into technical requirements. | Present |
| T0543 | **WITHDRAWN**: Use data carving techniques (e.g., FTK-Foremost) to extract data for further analysis. | Absent |

| | | |
|---|---|---|
| T0544 | Verify stability, interoperability, portability, and/or scalability of system architecture. | Present |
| T0545 | Work with stakeholders to resolve computer security incidents and vulnerability compliance. | Present |
| T0546 | Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies. | Present |
| T0547 | Research and evaluate available technologies and standards to meet customer requirements. | Absent |
| T0548 | Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. | Present |
| T0549 | 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 |
| T0550 | Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). | Present |
| T0551 | Draft and publish supply chain security and risk management documents. | Absent |
| T0552 | Review and approve a supply chain security/risk management policy. | Absent |
| T0553 | Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities. | Present |
| T0554 | Determine and document software patches or the extent of releases that would leave software vulnerable. | Absent |
| 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. | Present |
| T0556 | Assess and design security management functions as related to cyberspace. | Present |
| T0557 | Integrate key management functions as related to cyberspace. | Present |
| T0558 | Analyze user needs and requirements to plan and conduct system development. | Present |

| | | |
|---|---|---|
| T0559 | Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations. | Present |
| T0560 | Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information). | Absent |
| T0561 | Accurately characterize targets. | Absent |
| T0562 | Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements. | Present |
| T0563 | Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives. | Present |
| T0564 | Analyze feedback to determine extent to which collection products and services are meeting requirements. | Present |
| T0565 | Analyze incoming collection requests. | Absent |
| T0566 | Analyze internal operational architecture, tools, and procedures for ways to improve performance. | Absent |
| T0567 | Analyze target operational architecture for ways to gain access. | Present |
| T0568 | Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements). | Absent |
| T0569 | Answer requests for information. | Absent |
| T0570 | Apply and utilize authorized cyber capabilities to enable access to targeted networks. | Absent |
| T0571 | Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement. | Absent |
| T0572 | Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements. | Present |
| T0573 | Assess and apply operational environment factors and risks to collection management process. | Absent |

| | | |
|---|---|---|
| T0574 | Apply and obey applicable statutes, laws, regulations and policies. | Absent |
| T0575 | Coordinate for intelligence support to operational planning activities. | Present |
| T0576 | Assess all-source intelligence and recommend targets to support cyber operation objectives. | Absent |
| T0577 | Assess efficiency of existing information exchange and management systems. | Absent |
| T0578 | Assess performance of collection assets against prescribed specifications. | Present |
| T0579 | Assess target vulnerabilities and/or operational capabilities to determine course of action. | Present |
| T0580 | Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and adjust collection strategies and collection requirements accordingly. | Absent |
| T0581 | Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. | Absent |
| T0582 | Provide expertise to course of action development. | Present |
| T0583 | Provide subject matter expertise to the development of a common operational picture. | Present |
| T0584 | Maintain a common intelligence picture. | Absent |
| T0585 | Provide subject matter expertise to the development of cyber operations specific indicators. | Present |
| T0586 | Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Present |
| T0587 | Assist in the development and refinement of priority information requirements. | Present |
| T0588 | Provide expertise to the development of measures of effectiveness and measures of performance. | Absent |
| T0589 | Assist in the identification of intelligence collection shortfalls. | Present |
| T0590 | Enable synchronization of intelligence support plans across partner organizations as required. | Present |
| T0591 | Perform analysis for target infrastructure exploitation activities. | Absent |
| T0592 | Provide input to the identification of cyber-related success criteria. | Absent |
| T0593 | Brief threat and/or target current situations. | Present |
| T0594 | Build and maintain electronic target folders. | Absent |

| | | |
|---|---|---|
| T0595 | Classify documents in accordance with classification guidelines. | Absent |
| T0596 | Close requests for information once satisfied. | Present |
| T0597 | Collaborate with intelligence analysts/targeting organizations involved in related areas. | Present |
| T0598 | Collaborate with development organizations to create and deploy the tools needed to achieve objectives. | Absent |
| T0599 | Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas. | Absent |
| T0600 | Collaborate with other internal and external partner organizations on target access and operational issues. | Present |
| T0601 | Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials). | Present |
| T0602 | Collaborate with customer to define information requirements. | Present |
| T0603 | Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers. | Present |
| T0604 | Compare allocated and available assets to collection demand as expressed through requirements. | Present |
| T0605 | Compile lessons learned from collection management activity's execution of organization collection objectives. | Present |
| T0606 | Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. | Present |
| T0607 | Identify and conduct analysis of target communications to identify information essential to support operations. | Present |
| T0608 | Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access. | Absent |
| T0609 | Conduct access enabling of wireless computer and digital networks. | Absent |
| T0610 | Conduct collection and processing of wireless computer and digital networks. | Present |
| T0611 | Conduct end-of-operations assessments. | Absent |

| | | |
|---|---|---|
| T0612 | Conduct exploitation of wireless computer and digital networks. | Present |
| T0613 | Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures. | Present |
| T0614 | Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access. | Absent |
| T0615 | Conduct in-depth research and analysis. | Present |
| T0616 | Conduct network scouting and vulnerability analyses of systems within a network. | Present |
| T0617 | Conduct nodal analysis. | Absent |
| T0618 | Conduct on-net activities to control and exfiltrate data from deployed technologies. | Absent |
| T0619 | Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies. | Absent |
| T0620 | Conduct open source data collection via various online tools. | Absent |
| T0621 | Conduct quality control to determine validity and relevance of information gathered about networks. | Absent |
| T0622 | Develop, review and implement all levels of planning guidance in support of cyber operations. | Present |
| T0623 | Conduct survey of computer and digital networks. | Present |
| T0624 | Conduct target research and analysis. | Absent |
| T0625 | Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements. | Present |
| T0626 | Construct collection plans and matrixes using established guidance and procedures. | Present |
| T0627 | Contribute to crisis action planning for cyber operations. | Present |
| T0628 | Contribute to the development of the organization's decision support tools if necessary. | Absent |
| T0629 | Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers. | Absent |
| T0630 | Incorporate intelligence equities into the overall design of cyber operations plans. | Present |

| | | |
|---|---|---|
| T0631 | Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads. | Absent |
| T0632 | Coordinate inclusion of collection plan in appropriate documentation. | Absent |
| T0633 | Coordinate target vetting with appropriate partners. | Present |
| T0634 | Re-task or re-direct collection assets and resources. | Absent |
| T0635 | Coordinate with intelligence and cyber defense partners to obtain relevant essential information. | Present |
| T0636 | Coordinate with intelligence planners to ensure that collection managers receive information requirements. | Absent |
| T0637 | Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks. | Present |
| T0638 | Coordinate, produce, and track intelligence requirements. | Absent |
| T0639 | Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans. | Present |
| T0640 | Use intelligence estimates to counter potential target actions. | Present |
| T0641 | Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities. | Present |
| T0642 | Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology. | Absent |
| T0643 | Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers). | Absent |
| T0644 | Detect exploits against targeted networks and hosts and react accordingly. | Present |
| T0645 | Determine course of action for addressing changes to objectives, guidance, and operational environment. | Present |
| T0646 | Determine existing collection management webpage databases, libraries and storehouses. | Absent |
| T0647 | Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function. | Present |
| T0648 | Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives. | Present |

| | | |
|---|---|---|
| T0649 | Determine organizations and/or echelons with collection authority over all accessible collection assets. | Present |
| T0650 | Determine what technologies are used by a given target. | Present |
| T0651 | Develop a method for comparing collection reports to outstanding requirements to identify information gaps. | Present |
| T0652 | Develop all-source intelligence targeting materials. | Present |
| T0653 | Apply analytic techniques to gain more target information. | Absent |
| T0654 | Develop and maintain deliberate and/or crisis plans. | Absent |
| T0655 | Develop and review specific cyber operations guidance for integration into broader planning activities. | Present |
| T0656 | Develop and review intelligence guidance for integration into supporting cyber operations planning and execution. | Absent |
| T0657 | Develop coordinating instructions by collection discipline for each phase of an operation. | Present |
| T0658 | Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives. | Absent |
| T0659 | Develop detailed intelligence support to cyber operations requirements. | Absent |
| T0660 | Develop information requirements necessary for answering priority information requests. | Present |
| T0661 | Develop measures of effectiveness and measures of performance. | Absent |
| T0662 | Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis. | Present |
| T0663 | Develop munitions effectiveness assessment or operational assessment materials. | Present |
| T0664 | Develop new techniques for gaining and keeping access to target systems. | Absent |
| T0665 | Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations. | Present |
| T0666 | Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives. | Present |
| T0667 | Develop potential courses of action. | Absent |

| | | |
|---|---|---|
| T0668 | Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers. | Present |
| T0669 | Develop strategy and processes for partner planning, operations, and capability development. | Absent |
| T0670 | Develop, implement, and recommend changes to appropriate planning procedures and policies. | Present |
| T0671 | Develop, maintain, and assess cyber cooperation security agreements with external partners. | Absent |
| T0672 | Devise, document, and validate cyber operation strategy and planning documents. | Present |
| T0673 | Disseminate reports to inform decision makers on collection issues. | Absent |
| T0674 | Disseminate tasking messages and collection plans. | Absent |
| T0675 | Conduct and document an assessment of the collection results using established procedures. | Present |
| T0676 | Draft cyber intelligence collection and production requirements. | Absent |
| T0677 | Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems. | Present |
| T0678 | Engage customers to understand customers' intelligence needs and wants. | Present |
| T0679 | Ensure operational planning efforts are effectively transitioned to current operations. | Present |
| T0680 | Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines. | Absent |
| T0681 | Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems. | Present |
| T0682 | Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership. | Present |
| T0683 | Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures. | Present |
| T0684 | Estimate operational effects generated through cyber activities. | Present |
| T0685 | Evaluate threat decision-making processes. | Absent |
| T0686 | Identify threat vulnerabilities. | Present |
| T0687 | Identify threats to Blue Force vulnerabilities. | Absent |
| T0688 | Evaluate available capabilities against desired effects to recommend efficient solutions. | Absent |

| | | |
|---|---|---|
| T0689 | Evaluate extent to which collected information and/or produced intelligence satisfy information requests. | Absent |
| T0690 | Evaluate intelligence estimates to support the planning cycle. | Absent |
| T0691 | Evaluate the conditions that affect employment of available cyber intelligence capabilities. | Present |
| T0692 | Generate and evaluate the effectiveness of network analysis strategies. | Present |
| T0693 | Evaluate extent to which collection operations are synchronized with operational requirements. | Absent |
| T0694 | Evaluate the effectiveness of collection operations against the collection plan. | Absent |
| T0695 | Examine intercept-related metadata and content with an understanding of targeting significance. | Present |
| T0696 | Exploit network devices, security devices, and/or terminals or environments using various methods or tools. | Present |
| T0697 | Facilitate access enabling by physical and/or wireless means. | Absent |
| T0698 | Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers. | Absent |
| T0699 | Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives. | Absent |
| T0700 | Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community. | Absent |
| T0701 | Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development. | Present |
| T0702 | Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables. | Present |
| T0703 | Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities. | Present |
| T0704 | Incorporate cyber operations and communications security support plans into organization objectives. | Absent |

| | | |
|---|---|---|
| T0705 | Incorporate intelligence and counterintelligence to support plan development. | Present |
| T0706 | Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.) | Present |
| T0707 | Generate requests for information. | Absent |
| T0708 | Identify threat tactics, and methodologies. | Present |
| T0709 | Identify all available partner intelligence capabilities and limitations supporting cyber operations. | Present |
| T0710 | Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. | Absent |
| T0711 | Identify, draft, evaluate, and prioritize relevant intelligence or information requirements. | Absent |
| T0712 | Identify and manage security cooperation priorities with external partners. | Present |
| T0713 | Identify and submit intelligence requirements for the purposes of designating priority information requirements. | Absent |
| T0714 | Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups. | Absent |
| T0715 | Identify collection gaps and potential collection strategies against targets. | Present |
| T0716 | Identify coordination requirements and procedures with designated collection authorities. | Present |
| T0717 | Identify critical target elements. | Present |
| T0718 | Identify intelligence gaps and shortfalls. | Absent |
| T0719 | Identify cyber intelligence gaps and shortfalls for cyber operational planning. | Absent |
| T0720 | Identify gaps in our understanding of target technology and developing innovative collection approaches. | Absent |
| T0721 | Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness. | Present |
| T0722 | Identify network components and their functionality to enable analysis and target development. | Present |
| T0723 | Identify potential collection disciplines for application against priority information requirements. | Absent |
| T0724 | Identify potential points of strength and vulnerability within a network. | Absent |

| | | |
|---|---|---|
| T0725 | Identify and mitigate risks to collection management ability to support the plan, operations and target cycle. | Absent |
| T0726 | Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production. | Present |
| T0727 | Identify, locate, and track targets via geospatial analysis techniques. | Absent |
| T0728 | Provide input to or develop courses of action based on threat factors. | Absent |
| T0729 | Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities. | Absent |
| T0730 | Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures. | Absent |
| T0731 | Initiate requests to guide tasking and assist with collection management. | Present |
| T0732 | Integrate cyber planning/targeting efforts with other organizations. | Absent |
| T0733 | Interpret environment preparations assessments to determine a course of action. | Absent |
| T0734 | Issue requests for information. | Present |
| T0735 | Lead and coordinate intelligence support to operational planning. | Absent |
| T0736 | Lead or enable exploitation operations in support of organization objectives and target requirements. | Absent |
| T0737 | Link priority collection requirements to optimal assets and resources. | Present |
| T0738 | Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications. | Present |
| T0739 | Maintain relationships with internal and external partners involved in cyber planning or related areas. | Present |
| T0740 | Maintain situational awareness and functionality of organic operational infrastructure. | Present |
| T0741 | Maintain situational awareness of cyber-related intelligence requirements and associated tasking. | Absent |
| T0742 | Maintain situational awareness of partner capabilities and activities. | Present |

| | | |
|---|---|---|
| T0743 | Maintain situational awareness to determine if changes to the operating environment require review of the plan. | Absent |
| T0744 | Maintain target lists (i.e., RTL, JTL, CTL, etc.). | Absent |
| T0745 | Make recommendations to guide collection in support of customer requirements. | Present |
| T0746 | Modify collection requirements as necessary. | Present |
| T0747 | Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives. | Absent |
| T0748 | Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. | Present |
| T0749 | Monitor and report on validated threat activities. | Present |
| T0750 | Monitor completion of reallocated collection efforts. | Absent |
| T0751 | Monitor open source websites for hostile content directed towards organizational or partner interests. | Present |
| T0752 | Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements. | Absent |
| T0753 | Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture. | Absent |
| T0754 | Monitor target networks to provide indications and warning of target communications changes or processing failures. | Present |
| T0755 | Monitor the operational environment for potential factors and risks to the collection operation management process. | Absent |
| T0756 | Operate and maintain automated systems for gaining and maintaining access to target systems. | Absent |
| T0757 | Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements. | Absent |
| T0758 | 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 |
| T0759 | Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy. | Present |

| | | |
|---|---|---|
| T0760 | Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary. | Absent |
| T0761 | Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| T0762 | **WITHDRAWN:** Provide subject matter expertise in course of action development. | Present |
| T0763 | Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| T0764 | Provide subject matter expertise to planning efforts with internal and external cyber operations partners. | Present |
| T0765 | Provide subject matter expertise to development of exercises. | Present |
| T0766 | Propose policy which governs interactions with external coordination groups. | Present |
| T0767 | Perform content and/or metadata analysis to meet organization objectives. | Absent |
| T0768 | Conduct cyber activities to degrade/remove information resident in computers and computer networks. | Present |
| T0769 | Perform targeting automation activities. | Absent |
| T0770 | Characterize websites. | Absent |
| T0771 | Provide subject matter expertise to website characterizations. | Absent |
| T0772 | Prepare for and provide subject matter expertise to exercises. | Absent |
| T0773 | Prioritize collection requirements for collection platforms based on platform capabilities. | Present |
| T0774 | Process exfiltrated data for analysis and/or dissemination to customers. | Absent |
| T0775 | Produce network reconstructions. | Absent |
| T0776 | Produce target system analysis products. | Absent |
| T0777 | Profile network or system administrators and their activities. | Present |
| T0778 | Profile targets and their activities. | Absent |
| T0779 | Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations. | Absent |
| T0780 | Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans. | Absent |

| | | |
|---|---|---|
| T0781 | Provide aim point and reengagement recommendations. | Present |
| T0782 | Provide analyses and support for effectiveness assessment. | Present |
| T0783 | Provide current intelligence support to critical internal/external stakeholders as appropriate. | Present |
| T0784 | Provide cyber focused guidance and advice on intelligence support plan inputs. | Absent |
| T0785 | Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. | Absent |
| T0786 | Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. | Absent |
| T0787 | Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs. | Present |
| T0788 | Provide input and assist in post-action effectiveness assessments. | Absent |
| T0789 | Provide input and assist in the development of plans and guidance. | Absent |
| T0790 | Provide input for targeting effectiveness assessments for leadership acceptance. | Absent |
| T0791 | Provide input to the administrative and logistical elements of an operational support plan. | Absent |
| T0792 | Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations. | Absent |
| T0793 | Provide effectiveness support to designated exercises, and/or time sensitive operations. | Absent |
| T0794 | Provide operations and reengagement recommendations. | Absent |
| T0795 | Provide planning support between internal and external partners. | Absent |
| T0796 | Provide real-time actionable geolocation information. | Absent |
| T0797 | Provide target recommendations which meet leadership objectives. | Present |
| T0798 | Provide targeting products and targeting support as designated. | Absent |
| T0799 | Provide time sensitive targeting support. | Present |

| | | |
|---|---|---|
| T0800 | Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. | Present |
| T0801 | Recommend refinement, adaption, termination, and execution of operational plans as appropriate. | Present |
| T0802 | Review appropriate information sources to determine validity and relevance of information gathered. | Present |
| T0803 | Reconstruct networks in diagram or report format. | Present |
| T0804 | Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects. | Present |
| T0805 | Report intelligence-derived significant network events and intrusions. | Present |
| T0806 | Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures. | Present |
| T0807 | Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources. | Present |
| T0808 | Review and comprehend organizational leadership objectives and guidance for planning. | Present |
| T0809 | Review capabilities of allocated collection assets. | Absent |
| T0810 | Review intelligence collection guidance for accuracy/applicability. | Absent |
| T0811 | Review list of prioritized collection requirements and essential information. | Absent |
| T0812 | Review and update overarching collection plan, as required. | Absent |
| T0813 | Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities. | Present |
| T0814 | Revise collection matrix based on availability of optimal assets and resources. | Present |
| T0815 | Sanitize and minimize information to protect sources and methods. | Absent |
| T0816 | Scope the cyber intelligence planning effort. | Present |
| T0817 | Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations. | Absent |

| | | |
|---|---|---|
| T0818 | Serve as a liaison with external partners. | Absent |
| T0819 | Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements. | Absent |
| T0820 | Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources. | Present |
| T0821 | Specify discipline-specific collections and/or taskings that must be executed in the near term. | Present |
| T0822 | Submit information requests to collection requirement management section for processing as collection requests. | Present |
| T0823 | Submit or respond to requests for deconfliction of cyber operations. | Present |
| T0824 | Support identification and documentation of collateral effects. | Present |
| T0825 | Synchronize cyber international engagement activities and associated resource requirements as appropriate. | Present |
| T0826 | Synchronize cyber portions of security cooperation plans. | Present |
| T0827 | Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques. | Absent |
| T0828 | Test and evaluate locally developed tools for operational use. | Present |
| T0829 | Test internal developed tools and techniques against target tools. | Absent |
| T0830 | Track status of information requests, including those processed as collection requests and production requirements, using established procedures. | Absent |
| T0831 | Translate collection requests into applicable discipline-specific collection requirements. | Absent |
| T0832 | Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness. | Present |
| T0833 | Validate requests for information according to established criteria. | Present |
| T0834 | Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date. | Present |

| | | |
|---|---|---|
| T0835 | Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date. | Absent |
| T0836 | Document lessons learned that convey the results of events and/or exercises. | Absent |
| T0837 | Advise managers and operators on language and cultural issues that impact organization objectives. | Present |
| T0838 | Analyze and process information using language and/or cultural expertise. | Absent |
| T0839 | Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities. | Absent |
| T0840 | Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination. | Absent |
| T0841 | Conduct all-source target research to include the use of open source materials in the target language. | Absent |
| T0842 | Conduct analysis of target communications to identify essential information in support of organization objectives. | Present |
| T0843 | Perform quality review and provide feedback on transcribed or translated materials. | Absent |
| T0844 | Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing. | Absent |
| T0845 | Identify cyber threat tactics and methodologies. | Present |
| T0846 | Identify target communications within the global network. | Present |
| T0847 | Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis. | Absent |
| T0848 | Provide feedback to collection managers to enhance future collection and analysis. | Present |
| T0849 | Perform foreign language and dialect identification in initial source data. | Present |
| T0850 | Perform or support technical network analysis and mapping. | Present |
| T0851 | Provide requirements and feedback to optimize the development of language processing tools. | Absent |

| | | |
|---|---|---|
| T0852 | Perform social network analysis and document as appropriate. | Present |
| T0853 | Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material. | Absent |
| T0854 | Tip critical or time-sensitive information to appropriate customers. | Present |
| T0855 | Transcribe target voice materials in the target language. | Present |
| T0856 | Translate (e.g., verbatim, gist, and/or summaries) target graphic material. | Absent |
| T0857 | Translate (e.g., verbatim, gist, and/or summaries) target voice material. | Present |
| T0858 | Identify foreign language terminology within computer programs (e.g., comments, variable names). | Present |
| T0859 | Provide near-real time language analysis support (e.g., live operations). | Absent |
| T0860 | Identify cyber/technology-related terminology in the target language. | Present |
| T0861 | Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations. | Absent |
| T0862 | Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements. | Present |
| T0863 | Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner. | Absent |
| T0864 | Liaise with regulatory and accrediting bodies. | Present |
| T0865 | Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues. | Present |
| T0866 | Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance. | Absent |

| | | |
|---|---|---|
| T0867 | Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required. | Present |
| T0868 | Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues. | Absent |
| T0869 | Work with organization senior management to establish an organization-wide Privacy Oversight Committee | Present |
| T0870 | Serve in a leadership role for Privacy Oversight Committee activities | Absent |
| T0871 | Collaborate on cyber privacy and security policies and procedures | Present |
| T0872 | Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation | Absent |
| T0873 | Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations | Absent |
| T0874 | Provide strategic guidance to corporate officers regarding information resources and technology | Present |
| T0875 | Assist the Security Officer with the development and implementation of an information infrastructure | Absent |
| T0876 | Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations. | Absent |
| T0877 | Work cooperatively with applicable organization units in overseeing consumer information access rights | Absent |
| T0878 | Serve as the information privacy liaison for users of technology systems | Present |
| T0879 | Act as a liaison to the information systems department | Present |
| T0880 | Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations | Absent |
| T0881 | Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, | Present |

| | | |
|---|---|---|
| | volunteers, contractors, alliances, business associates and other appropriate third parties | |
| T0882 | Conduct on-going privacy training and awareness activities | Present |
| T0883 | Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security | Present |
| T0884 | Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard. | Absent |
| T0885 | Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee | Absent |
| T0886 | Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data | Present |
| T0887 | Provide leadership for the organization's privacy program | Absent |
| T0888 | Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization | Present |
| T0889 | Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable | Present |
| T0890 | Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures | Absent |
| T0891 | Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices | Present |
| T0892 | Develop and coordinate a risk management and compliance framework for privacy | Absent |

| | | |
|---|---|---|
| T0893 | Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies. | Present |
| T0894 | Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations | Absent |
| T0895 | Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization's privacy policies and procedures | Absent |
| T0896 | Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity | Absent |
| T0897 | Provide leadership in the planning, design and evaluation of privacy and security related projects | Present |
| T0898 | Establish an internal privacy audit program | Present |
| T0899 | Periodically revise the privacy program considering changes in laws, regulatory or company policy | Absent |
| T0900 | Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel | Present |
| T0901 | Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information | Present |
| T0902 | Monitor systems development and operations for security and privacy compliance | Present |
| T0903 | Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected | Present |
| T0904 | Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions | Absent |
| T0905 | Review all system-related information security plans to ensure alignment between security and privacy practices | Absent |

| | | |
|---|---|---|
| T0906 | Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements | Absent |
| T0907 | Account for and administer individual requests for release or disclosure of personal and/or protected information | Present |
| T0908 | Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements | Absent |
| T0909 | Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed | Present |
| T0910 | Act as, or work with, counsel relating to business partner contracts | Absent |
| T0911 | Mitigate effects of a use or disclosure of personal information by employees or business partners | Absent |
| T0912 | Develop and apply corrective action procedures | Absent |
| T0913 | Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel | Absent |
| T0914 | Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations | Absent |
| T0915 | Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations | Absent |
| T0916 | Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units | Absent |
| T0917 | Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices | Present |
| T0918 | Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations | Present |

| | | |
|---|---|---|
| T0919 | Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials | Present |
| T0920 | Develop and maintain appropriate communications and training to promote and educate all workforce members and members of the Board regarding privacy compliance issues and requirements, and the consequences of noncompliance | Absent |
| T0921 | Determine business partner requirements related to the organization's privacy program. | Absent |
| T0922 | Establish and administer a process for receiving, documenting, tracking, investigating and taking corrective action as appropriate on complaints concerning the company's privacy policies and procedures. | Present |
| T0923 | Cooperate with the relevant regulatory agencies and other legal entities, and organization officers, in any compliance reviews or investigations. | Present |
| T0924 | Perform ongoing privacy compliance monitoring activities. | Present |
| T0925 | Monitor advancements in information privacy technologies to ensure organization adoption and compliance. | Absent |
| T0926 | 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 |
| T0927 | Appoint and guide a team of IT security experts. | Present |
| T0928 | Collaborate with key stakeholders to establish a cybersecurity risk management program. | Absent |
| T0929 | Identify and assign individuals to specific roles associated with the execution of the Risk Management Framework. | Present |
| T0930 | Establish a risk management strategy for the organization that includes a determination of risk tolerance. | Absent |
| T0931 | Identify the missions, business functions, and mission/business processes the system will support. | Absent |
| T0932 | Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system. | Present |

| | | |
|---|---|---|
| T0933 | Identify stakeholders who have a security interest in the development, implementation, operation, or sustainment of a system. | Present |
| T0934 | Identify stakeholder assets that require protection. | Absent |
| T0935 | Conduct an initial risk assessment of stakeholder assets and update the risk assessment on an ongoing basis. | Absent |
| T0936 | Define the stakeholder protection needs and stakeholder security requirements. | Absent |
| T0937 | Determine the placement of a system within the enterprise architecture. | Absent |
| T0938 | Identify organization-wide common controls that are available for inheritance by organizational systems. | Absent |
| T0939 | Conduct a second-level security categorization for organizational systems with the same impact level. | Present |
| T0940 | Determine the boundary of a system. | Present |
| T0941 | Identify the security requirements allocated to a system and to the organization. | Absent |
| T0942 | Identify the types of information to be processed, stored, or transmitted by a system. | Absent |
| T0943 | Categorize the system and document the security categorization results as part of system requirements. | Absent |
| T0944 | Describe the characteristics of a system. | Present |
| T0945 | Register the system with appropriate organizational program/management offices. | Absent |
| T0946 | Select the security controls for a system and document the functional description of the planned control implementations in a security plan. | Absent |
| T0947 | Develop a strategy for monitoring security control effectiveness; coordinate the system-level strategy with the organization and mission/business process-level monitoring strategy. | Present |
| T0948 | Review and approve security plans. | Absent |
| T0949 | Implement the security controls specified in a security plan or other system documentation. | Present |
| T0950 | Document changes to planned security control implementation and establish the configuration baseline for a system. | Present |
| T0951 | Develop, review, and approve a plan to assess the security controls in a system and the organization. | Present |

| | | |
|---|---|---|
| T0952 | Assess the security controls in accordance with the assessment procedures defined in a security assessment plan. | Present |
| T0953 | Prepare a security assessment report documenting the issues, findings, and recommendations from the security control assessment. | Absent |
| T0954 | Conduct initial remediation actions on security controls based on the findings and recommendations of a security assessment report; reassess remediated controls. | Present |
| T0955 | Prepare a plan of action and milestones based on the findings and recommendations of a security assessment report excluding any remediation actions taken. | Absent |
| T0956 | Assemble an authorization package and submit the package to an authorizing official for adjudication. | Absent |
| T0957 | Determine the risk from the operation or use of a system or the provision or use of common controls. | Absent |
| T0958 | Identify and implement a preferred course of action in response to the risk determined. | Absent |
| T0959 | Determine if the risk from the operation or use of the system or the provision or use of common controls, is acceptable. | Absent |
| T0960 | Monitor changes to a system and its environment of operation. | Absent |
| T0961 | Assess the security controls employed within and inherited by the system in accordance with an organization-defined monitoring strategy. | Present |
| T0962 | Respond to risk based on the results of ongoing monitoring activities, assessment of risk, and outstanding items in a plan of action and milestones. | Absent |
| T0963 | Update a security plan, security assessment report, and plan of action and milestones based on the results of a continuous monitoring process. | Absent |
| T0964 | Report the security status of a system (including the effectiveness of security controls) to an authorizing official on an ongoing basis in accordance with the monitoring strategy. | Present |
| T0965 | Review the security status of a system (including the effectiveness of security controls) on an ongoing basis to determine whether the risk remains acceptable. | Absent |

| | | |
|---|---|---|
| T0966 | Implement a system disposal strategy which executes required actions when a system is removed from service. | Absent |
| T0967 | Sponsor and promote continuous monitoring within the organization. | Absent |
| T0968 | Assign staff as needed to appropriate continuous monitoring working groups. | Absent |
| T0969 | Identify reporting requirements to support continuous monitoring activities. | Absent |
| T0970 | Establish scoring and grading metrics to measure effectiveness of continuous monitoring program. | Absent |
| T0971 | Determine how to integrate a continuous monitoring program into the organization's broader information security governance structures and policies. | Present |
| T0972 | Use continuous monitoring scoring and grading metrics to make information security investment decisions to address persistent issues. | Present |
| T0973 | Ensure that the continuous monitoring staff have the training and resources (e.g., staff and budget) needed to perform assigned duties. | Absent |
| T0974 | Work with organizational risk analysts to ensure that continuous monitoring reporting covers appropriate levels of the organization. | Absent |
| T0975 | Work with the organizational risk analysts to ensure risk metrics are defining realistically to support continuous monitoring. | Absent |
| T0976 | Work with organizational officials to ensure continuous monitoring tool data provides situation awareness of risk levels. | Absent |
| T0977 | Establish triggers for unacceptable risk thresholds for continuous monitoring data. | Present |
| T0978 | Work with organizational officials to establish system level reporting categories that can be used by the organization's continuous monitoring program. | Present |
| T0980 | Designate a qualified person to be responsible for the management and implementation of the continuous monitoring program. | Present |
| T0981 | Identify the continuous monitoring stakeholders and establish a process to keep them informed about the program. | Absent |
| T0982 | Identify security oriented organization reporting requirements that are fulfilled by the continuous monitoring program. | Absent |

| | | |
|---|---|---|
| T0983 | Use the continuous monitoring data to make information security investment decisions to address persistent issues. | Present |
| T0984 | Define triggers within the continuous monitoring program that can be used to define unacceptable risk and result in action being taken to resolve. | Present |
| T0985 | Establish scoring and grading metrics to measure effectiveness of continuous monitoring program. | Present |
| T0986 | Work with security managers to establish appropriate continuous monitoring reporting requirements at the system level. | Absent |
| T0987 | Use the continuous monitoring tools and technologies to assess risk on an ongoing basis. | Present |
| T0988 | Establish appropriate reporting requirements in adherence to the criteria identified in the continuous monitoring program for use in automated control assessment. | Present |
| T0989 | Use non-automated assessment methods where the data from the continuous monitoring tools and technologies is not yet of adequate sufficiency or quality. | Present |
| T0990 | Develop processes with the external audit group on how to share information regarding the continuous monitoring program and its impact on security control assessment. | Absent |
| T0991 | Identify reporting requirements for use in automated control assessment to support continuous monitoring. | Absent |
| T0992 | Determine how the continuous monitoring results will be used in ongoing authorization. | Absent |
| T0993 | Establish continuous monitoring tools and technologies access control process and procedures. | Absent |
| T0994 | Ensure that continuous monitoring tools and technologies access control is managed adequately. | Absent |
| T0995 | Establish a process to provide technical help to continuous monitoring mitigators. | Absent |
| T0996 | Coordinate continuous monitoring reporting requirements across various users. | Absent |
| T0997 | Establish responsibilities for supporting implementation of each continuous monitoring tool or technology. | Present |

| | | |
|---|---|---|
| T0998 | Establish liaison with scoring and metrics working group to support continuous monitoring. | Present |
| T0999 | Establish and operate a process to manage introduction of new risk to support continuous monitoring. | Present |
| T1000 | Establish continuous monitoring configuration settings issues and coordination sub-group. | Present |
| T1001 | Establish continuous monitoring tools and technologies performance measurement/management requirements. | Absent |
| T1002 | Using scores and grades to motivate and assess performance while addressing concerns to support continuous monitoring | Absent |
| T1003 | Work with security managers (i.e., system owners, information system security managers, information system security officers, etc.) to establish appropriate reporting requirements for continuous monitoring at the system level. | Present |
| T1004 | Use continuous monitoring tools to assess risk on an ongoing basis. | Present |
| T1005 | Use the continuous monitoring data to make information security investment decisions to address persistent issues. | Absent |
| T1006 | Respond to issues flagged during continuous monitoring, escalate and coordinate a response. | Present |
| T1007 | Review findings from the continuous monitoring program and mitigate risks on a timely basis. | Present |

g. List of potential threats to Secure Systems that could exploit vulnerabilities of critical assets due
to missing Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks

- Unauthorized access
- Bugs in source code and software
- Unauthorized access
- Administrative access to modify the mail server
- Disgruntled employee

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

- Leaked PII data
- Ransomware
- Remote code execution
- Disabling or crashing the system
- Leaked confidential financial data
- DOS threats
- Leaked confidential emails
- Leaking confidential company data
- Whistleblowers

i. List of recommended policies (Hiring new Cybersecurity staff, Educating current staff, Outsourcing) for each recommended Cybersecurity Specialty Area, Cybersecurity Work Role, or Cybersecurity Task that should be created to mitigate the identified risks (it is not required to write detailed policies

- Regular training for all the employees on phishing and social engineering attacks should be provided.
- Maintaining positive work culture in the workplace and good relationship between manager and employees is important for retention of great employees.
- External audit or pen testing teams can work closely with internal teams to improve the security posture of the organization.
- Educating employees on how to store and manage their credentials safely and how to regularly update their passwords is important
- Prioritizing vulnerability management and keeping the systems up to date with latest security patches is important.
- Access control both physically and logically can be made stricter so that critical data is not leaked.
- Source code validation using static analyzers, code reviews can be prioritized higher than what it already is.

# Part C

C1. Security Risk Management Recommendations: Provide the list of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits based on your risk management analysis in Parts A and B above

For HGA:

- Mixed strategy can be the best option considering the evolution of threat vectors every day.
- Mixed strategy also has the best cost-benefit ratio which makes it more meaningful
- Prioritizing controls which add the highest value in protecting critical assets to incorporate new changes suggested can be the best viable option:
    1. COG contingency planning
    2. Protection against disclosure of information
    3. Protection against network related attacks

For Secure Systems:

- Implementing strict access control mechanism to allow access to employees and customer PII
- Encrypting the data with the latest and great cryptographic algorithms
- Static and dynamic code analysis before source code/software is deployed in productions
- Red teaming to identify vulnerabilities from an attacker perspective
- Hardening access to the mail server and implementing strict access control mechanisms
- Using SMIME for confidential emails
- Treating all employees with respect and dignity - important in work culture
- Store only data that is necessary
- Delete unnecessary data
- Avoid storing source code in vulnerable systems
- Have a protected centralized repository for source code and software
- Training for developers on how to handle source code and software securely
- Store only necessary data and delete the rest
- Education employees dealing with financial data about best practices and risks
- No single point of failure
- Periodic maintenance of servers with latest updates
- Having a transparent and open culture
- Third-party and independent reviews to understand and address employee concerns

C2. Provide the total cost and benefit in $ for the recommended controls, methods and policies based on your security risk management analysis in Parts A and B above

For HGA:

**Cost-benefit ratio analysis for Risk Prevention budget**

Total Asset value for chosen assets = $3,650,000
Total Residual risk for assets after implementing risk analysis = $1,095,000
Expected Security risk-benefit = $2,555,000

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 1,550,000/2,555,000
  = 0.606

**Cost-benefit ratio analysis for Risk Response budget**

Total Asset value for chosen assets = $3,650,000
Total Residual risk for assets after implementing risk analysis = $229,960
Expected Security risk-benefit = $3,420,040

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 1,600,000/3,420,040
  = 0.468

**Cost-benefit ratio analysis for Mixed strategy budget**

Total Asset value for chosen assets = $3,650,000
Total Residual risk for assets after implementing risk analysis = $50,735
Expected Security risk-benefit = $3,599,265

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 2,450,000/3,599,265
  = 0.681

For SecureSystems:

**Cost-benefit ratio analysis for Risk Prevention budget**

Total Asset value for chosen assets = $230,000,000
Total Residual risk for assets after implementing risk analysis = $50,000,000
Expected Security risk-benefit = $180,000,000

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 125,000,000/180,000,000
  = 0.694

**Cost-benefit ratio analysis for Risk Response budget**

Total Asset value for chosen assets = $230,000,000
Total Residual risk for assets after implementing risk analysis = $80,000,000
Expected Security risk-benefit = $150,000,000

- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 115,000,000/150,000,000
  = 0.766

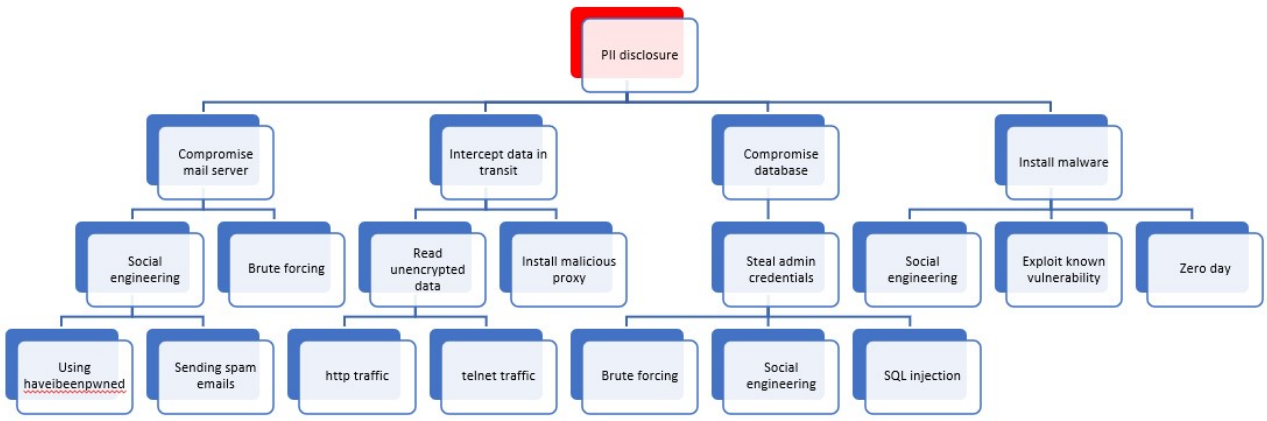
**Cost-benefit ratio analysis for Mixed strategy budget**

Total Asset value for chosen assets = $230,000,000
Total Residual risk for assets after implementing risk analysis = $30,000,000
Expected Security risk-benefit = $200,000,000

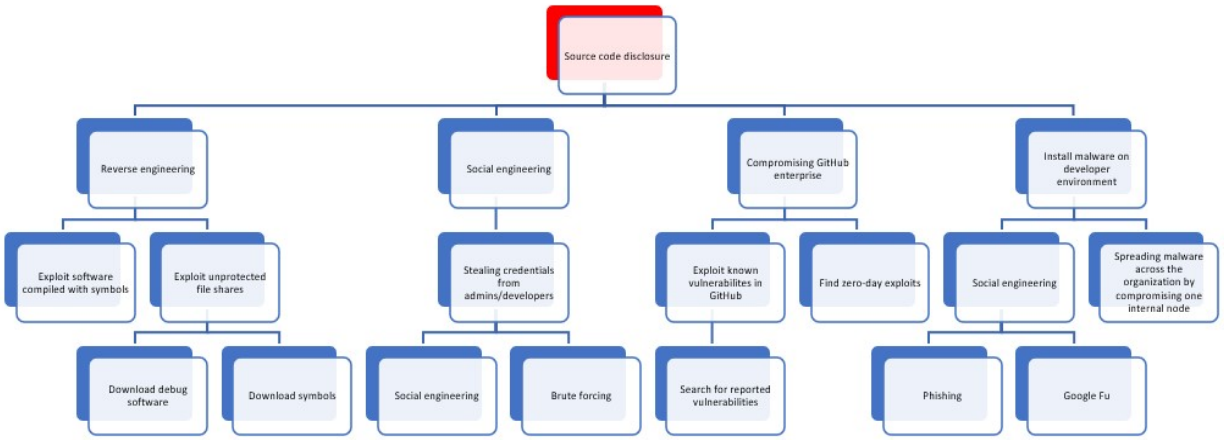
- Proposed security risk budget cost / Expected Security Risk-Benefit
  = 170,000,000/200,000,000
  = 0.85

| Points of consideration | HGA | Secure Systems |
|---|---|---|
| Industry | Payroll – government | Endpoint security - private |
| Mission | Managing payroll and financial details of government agencies | To provide various product offerings for corporate endpoint security |
| Geographic presence | USA | Worldwide |
| Number of employees | 1000 | 7500 |
| Network topology | Appendix 3 | Appendix 4 |
| Critical Assets $ | $3,650,000 | $230,000,000 |
| Threat environment | Nation state, insider threats, cyber criminals | Competitors, hackers, insider threats, malware |
| Residual security risk $ | $50,735 | $3,000,000 |
| Budget for risk prevention and response controls | $2,450,000 | $170,000,000 |
| - $ security budget / $ security risk improvement | 0.681 | 0.85 |
| $ security budget / $ critical assets | 0.67 | 0.74 |
| $ security budget / employee | $2450 | $22666 |

Attack tree for HGA



Attack tree for Secure Systems




Vulnerabilities and Exploitation Probabilities

For HGA:

| Vulnerability | Exploitation probability |
|---|---|
| V1.1: Falsified Time Sheets | 55 |
| V1.2: Unauthorized Access | 60 |
| V1.3: Bogus Time and Attendance Applications | 45 |
| V1.4: Unauthorized Modifications of Time and Attendance Sheets | 35 |
| V2: Vulnerabilities Related to Payroll Errors - late submission of personnel paperwork | 50 |
| V3.1: COG Contingency Planning - improper verification | 55 |
| V3.2: Division Contingency Planning - improper delegation to COG | 65 |
| V3.3: Virus Prevention | 40 |
| V3.4: Accidental Corruption and Loss of Data | 55 |
| V4: Vulnerabilities Related to Disclosure or Brokerage of information - improper logins and sniffer programs | 60 |
| V5: Vulnerabilities Related to Network-Related Attacks - email utility vulnerability and eavesdropping | 50 |

For Secure Systems:

| **Vulnerabilities** | Exploitation probability |
|---|---|
| Unauthorized access | 60 |
| Bugs in source code and software | 70 |
| Unauthorized access | 65 |
| Administrative access to modify the mail server | 60 |
| Disgruntled employee | 70 |

**Cybersecurity workforce recommendations**

For HGA:

- Regular training for all the employees on phishing and social engineering attacks should be provided.
- Hiring more employees on identity and access management roles (IAM).
- Educating employees on how to store and manage their credentials safely and how to regularly update their passwords is important
- Hiring developers and security engineers to keep the payroll software up-to-date and free from any security vulnerabilites
- Improving the incident response and contingency planning team
- Hiring more network security engineers to prevent any network security related attacks.

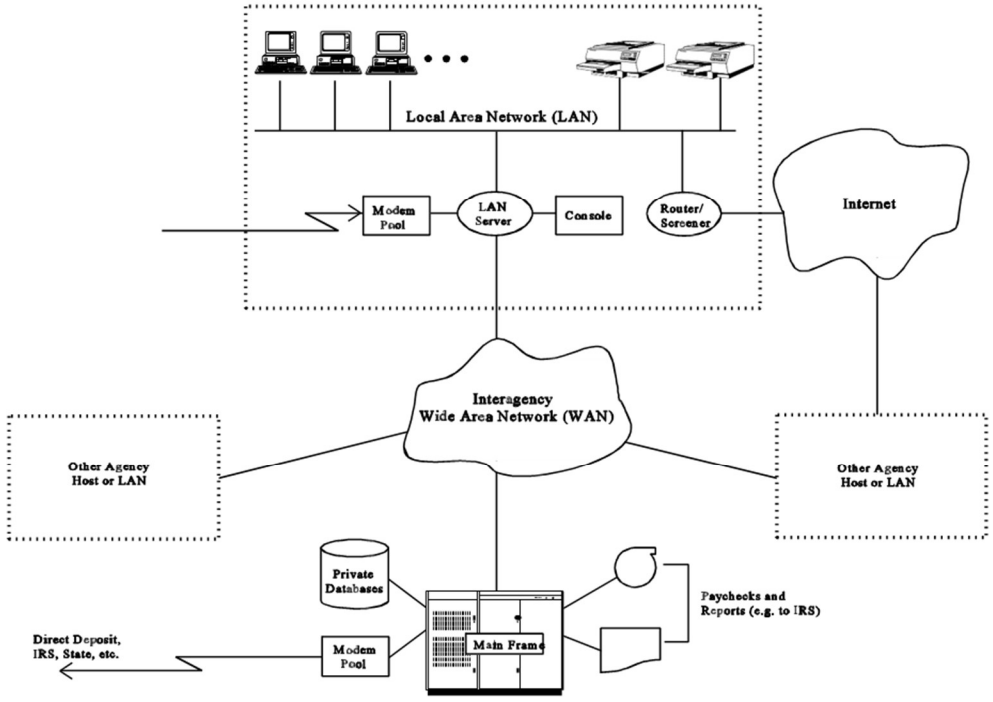
For SecureSystems:

- Regular training for all the employees on phishing and social engineering attacks should be provided.
- Maintaining positive work culture in the workplace and good relationship between manager and employees is important for retention of great employees.
- External audit or pen testing teams can work closely with internal teams to improve the security posture of the organization.
- Educating employees on how to store and manage their credentials safely and how to regularly update their passwords is important

- Prioritizing vulnerability management and keeping the systems up to date with latest security patches is important.
- Access control both physically and logically can be made stricter so that critical data is not leaked.
- Source code validation using static analyzers, code reviews can be prioritized higher than what it already is.

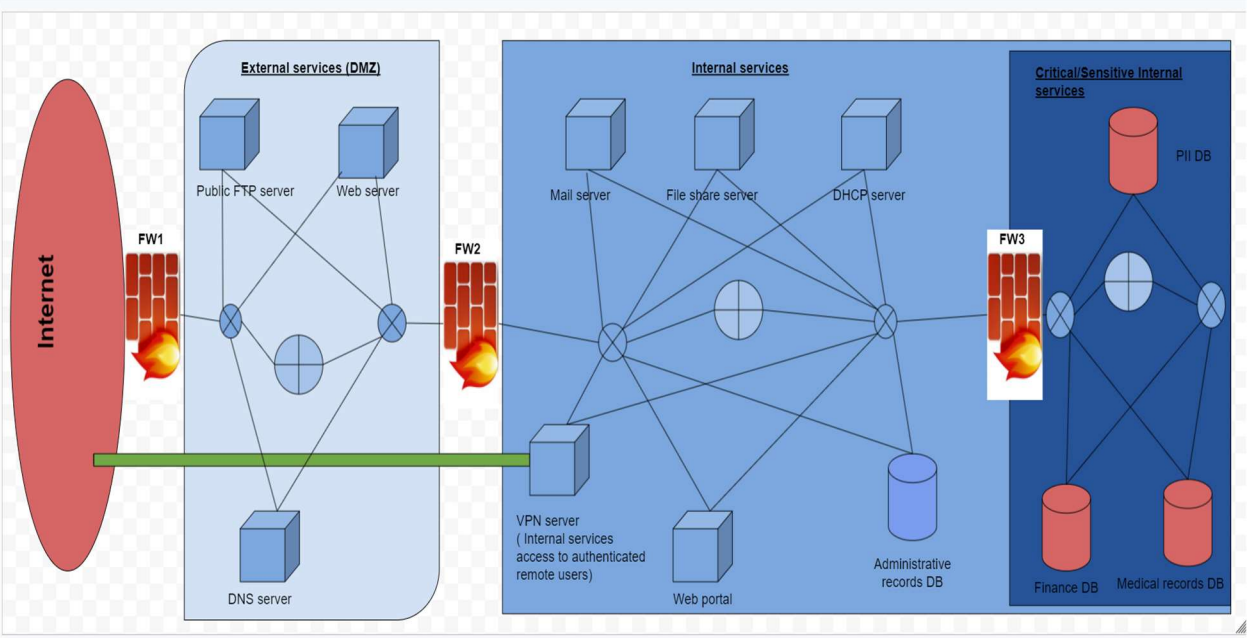
# Part D

**Appendix 3: Detailed Network Topology for HGA Appendix**




The environment shows the Wide Area Network (WAN) which connects all the agencies which have their own Local Area Networks( LAN). The mainframe computer is connected to the private database and the modem pool. It also has paychecks and reports regarding the organization.

**Appendix 4: Detailed Network Topology (defense-in-depth) for Secure Systems**




Sample organization network diagram for SecureSystems. It implements the defense-in-depth approach for network security.
There are multiple firewalls to secure services/data across various levels. DMZ is facing the external network which is the internet and it's protected by just one basic firewall. To access the internal network and critical internal network, users have to go through multiple firewalls and access control checks thereby implementing the defense-in-depth approach.

It is very hard for the attacker to access critical internal services as he/she has to go through three checks to gain that access.

## References


- https://en.wikipedia.org/wiki/Risk_Management_Framework

  https://www.cybergrx.com/resources/research-and-insights/blog/internet-of-things-iot-devices-third-party-cyber-risk-management

- https://owasp.org/www-project-top-ten/

- https://www.palisade.com/risk/monte_carlo_simulation.asp

- https://www.techtarget.com/searchsecurity/tip/IPSec-VPN-vs-SSL-VPN-Comparing-respective-VPN-security-risks

- https://www.apriorit.com/dev-blog/676-cybersecurity-risk-assessment-with-pentesting

- https://www.isaca.org/resources/isaca-journal/issues/2017/volume-3/it-asset-valuation-risk-assessment-and-control-implementation-model#:~:text=Asset%20Valuation,-This%20is%20a&text=CIA%20of%20information%20will%20have,%2B%20I%20%2B%20A)%20attributes.

- https://www.security7.net/news/the-7-steps-of-a-successful-risk-assessment

- https://www.pmlearningsolutions.com/blog/qualitative-risk-analysis-vs-quantitative-risk-analysis-pmp-concept-1