**CY 5200 Security Risk Management and Assessment**

**Instructor: Prof. Themis A. Papageorge**

**Student: Avinash Nutalapati**

**Text

Description automatically generated**

**Text, whiteboard

Description automatically generated**

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Part** | **Title** | **Pg. No** |
| **Part A** | Security Risk Management Assessment |  |
| Executive summary | 6 |
| List of Assets with Values (S) | 11 |
| List of Threats | 12 |
| List of Vulnerabilities | 13 |
| Threat/Vulnerability pairs | 13 |
| Assets impacted by Threat/Vulnerability pairs | 13 |
| MOT — which MOT controls are covered by current HGA controls | 18 |
| MOT - proposed by new CISO HGA controls AND VPN server AND DMZ | 19 |
| Security Risk Prevention Strategy | 20 |
| Security Risk Response (Resilience) Strategy | 24 |
| Mixed Security Risk Prevention Strategy and Security Risk Response (Resilience) Strategy | 37 |
| Conclusion: Cost Benefit Analysis | 40 |
| **Part B** | Security Risk Management Implementation Plan | 43 |
| Access Control Security Risk Management Implementation Controls and Policies | 44 |
| Network Infrastructure Security Risk Management Implementation Controls and Policies | 45 |
| Network Infrastructure Management Security Risk Management Implementation Controls and Policies | 46 |
| Database Security Risk Management Implementation Controls and Policies | 48 |
| Applications Development Security Risk Management Implementation Controls and Policies | 50 |
| Wireless Security Risk Management Implementation Controls and Policies | 51 |
| List of Cybersecurity Implementation controls that exist at Pearson Specter LLP | 53 |
| Comparison of the Implementation controls discussed in class with Pearson Specter LIP's existing Cybersecurity Implementation controls | 54 |
| List of critical assets that exist in Pearson Specter LLP | 54 |
| List of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing | 68 |
| List of potential threats to Pearson Specter LLP that could exploit vulnerabilities Of critical assets | 68 |
| List of potential risks for critical assets where Cybersecurity Implementation Controls are missing | 68 |
| List of recommended Hardening Prevention controls and policies | 69 |
| List of recommended Hardening Response controls and policies for critical assets | 69 |
| Applicable Government Regulations and Industry Standards | 70 |
| Rank asset risks and vulnerability risks | 76 |
| List of Cybersecurity Specialty Areas that exist in Pearson Specter LLP | 79 |
| List of Cybersecurity Work Roles that exist in Pearson Specter LLP | 81 |
| List of Cybersecurity Tasks that exist in Pearson Specter LLP | 81 |
| Comparison of the NCWF recommended Cybersecurity Specialty Areas with Pearson Specter LLP's existing Cybersecurity Specialty Areas | 90 |
| Comparison of the NCWF recommended Cybersecurity Work Roles with Pearson Specter | 91 |
| LLP's existing Cybersecurity Work Roles | 91 |
| Comparison the NCWF recommended Cybersecurity Tasks with Pearson Specter LIP's existing | 91 |
| Cybersecurity Tasks | 91 |
| List of potential threats to Pearson Specter LIP that could exploit vulnerabilities of critical assets | 162 |
| List of potential risks for critical assets where Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks are missing | 163 |
| List of recommended policies that should be created to mitigate the identified risks | 163 |
| **Part C** | Security Risk Management Recommendations | 164 |
| List of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits | 164 |
| Provide the total cost and benefit in $ | 165 |
| Compare your proposed security controls, methods and policies budget for HCA with the proposed security controls, methods and policies budget for Pearson Specter LLP | 167 |
| Attack Tree for HGA | 168 |
| Attack Tree for Pearson Specter LLP | 169 |
| Vulnerabilities and Exploitation Probabilities | 169 |
| Cybersecurity Workforce Recommendation | 170 |
| **Part D** | Appendix | 172 |
| Appendix 3: Detailed Network Topology for HGA | 173 |
| Appendix 4: Detailed Network Topology (defense-in-depth) for Pearson Specter LLP | 174 |
| References | 175 |

**Part A: Security Risk Management Assessment**

**Executive Summary:**

**Information System Name:** Hypothetical Government Agency

**Information System Categorization:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Assets** | Information security Elements | | |
| **Confidentiality (C)** | **Integrity (I)** | **Availability (A)** |
| Financial Resources | High | High | High |
| Systems and its components | High | High | High |
| Contracting and Procurement Documents | High | High | High |
| Internal Correspondence & Draft Regulations | High | High | High |
| Servers | High | High | High |
| Special Administrative Console | High | High | High |
| Personal Information | High | High | High |

**Organization Name:** Hypothetical Government Agency

**Organization Address:** 11 Wall St, Boston, MA 02125

**Abhinav Singari**

**Title**: Chief Executive Officer (President)

**Email**: [**abhinav.singari@hga.gov**](mailto:abhinav.singari@hga.gov)

**Phone**: +1 617 764583

**David Rockwell**

**Title**: Chief Information Officer

**Email**: [**david.rockwell1@hga.gov**](mailto:david.rockwell1@hga.gov)

**Phone**: +1 617 546736

**Maxwell Gilbert**

**Title**: Chief Financial Officer

**Email**: [**g.maxwell@hga**](mailto:g.maxwell@hga)**.gov**

**Phone**: +1 617 8764536

**Russel Goran**

**Title**: Chief Information Security Officer

**Email**: [**goranrussel@hga.**](mailto:goranrussel@hga.)**gov**

**Phone**: +1 617 863453

**Shankar Natraj**

**Title**: Chief Infrastructure Officer (Vice President)

**Email**: [**natraj.shankar@hga.gov**](mailto:natraj.shankar@hga.gov)

**Phone**: +1 617 120983

**Information System Operational Status:** Operational

**Information System Type:** Major Application

**System Description**: Funds Transfer from the US Government to Individual Consumers

**HGA System Infrastructure and Network Topology:**



The network topology of the HGA can be explained considering the most critical and central part of it, which is WAN (Wide Area Network). WAN is integrating the LAN of HGA to the Other agency LAN networks and to the private database and model pool. Within the HGA LAN, it is connected to an administrative console and modem pool along with the critical infrastructure of HGA such as its systems, servers, and printers. This type of connection is very practical and most effective in terms of security as the internal network is isolated from the external and centralized components manages the network traffic without impacting the critical infrastructure.

**Interconnection of System Information:**

**System Name:** Government Agency

**Type Of Organization**: Public Sector Telecommunication Industry

**Type of Agreement:** Government Contract

**Date:** March 31, 1993

**FIPS 199 category:** High (H)

**Category:** Accredited and Certified

**Authorizing Official:** Karuna Rathod

**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 Controls** | **Observations** | **Status** | **Control Type** | **Responsible Authority** |
| Separation of Duties (M1) | Division of work among the infrastructure and security teams. Proper communication among the teams and schedules of any deployments in regards to interdependency must be communicated. | Partial | Common | CIO |
| Business Continuity Plans (M2) | In the event of black swan events or any type of unexpected, delayed process, business and security must continue and the team is working on this. | Partial | Common | CIO |
| Dedicated Incident Response Team (M3) | Establishment of the SOC team is on the way and L1 and L2 teams have been identified for proper escalations. | Complete | Common | CISO |
| Compliance Audits (M4) | Frequent auditing of the work process being followed and audits during new project implementation are underway. Need to figure out other possible ways of effective auditing. | Partial | Common | CISO |
| Contingency Planning (M5) | Contingency Plans have been placed to compensate for any type of work balance and dependencies. | Complete | Common | CIO |
| Security Training for Employees (M6) | Security training regarding Phishing mail detection and password protection is completed. There is still furthermore training to enhance the physical security and shoulder surfing activities. | Partial | Common | CISO |
| Security Policy review (M7) | CISO and new security have reviewed all the current security policies and proposed new policies. | Complete | Common | CISO |
| Data Classification and Backups (M8) | Infrastructure teams and server team has finalized the threshold required for backups and the process has been identified. | Partial | Common | CIO |
| Physical Security of Assets (M9) | Cameras-monitoring, regular employee bag checks, and workspace security have been in place. | Complete | Common | CIO |
| Security Audits (M10) | The security team conducts security audits project-wise and check for any possible leakage of passwords or any documents left unsecured will be identified. Any communication made to personal mails will be identified here. | Complete | Common | CISO |
| Data Loss Prevention techniques (M11) | IDP and IDS methods were included in the SIEM so that any ransomware attacks can be identified, and internal threats are closely monitored. | Complete | Common | CISO |
| Identity access management controls (M12) | New security tools like One trust, CyberArk are considered to improve the IAM of HGA. | Partial | Common | CISO |
| Network traffic monitoring (M13) | Firewalls are considered and integration of firewall traffic to SIEM will be enabled soon. | Partial | Common | CISO |
| Automated fraudulence payroll detectors (M14) | There are software available to check suspicious payroll activities and random manual checks of payrolls are considered. | Complete | Common | CIO |
| Threat Intelligence & Reports (M15) | 3rd party TI or open-source TI are used to identify the threats and CIO and their teams help the security team to identify any affected products in the HGA environment. | Complete | Common | CISO |

Information Security Plan Completion Date: 09/03/2022

Information Security Plan Approval Date: 12/12/2022

**Class Assignment – HGA Case Study – Risk Analysis**

**Security Risk Analysis of HGA**

The below document is the Security Risk Analysis of HGA Case Study.

Firstly, the list of assets, threats associated, and vulnerabilities are listed, and the security assessments are done before and after each strategy has been applied. There are 3 scenarios considered here and a plan for resilience and the security risk assessment after the implementation of organization-level strategies are considered. Please follow the below document for a detailed analysis report.

**Information of Assets:**

The total employee count of HGA could be determined as 300. All the employees and associated agency data are considered as highly sensitive data which when valued is estimated at $330000 and the financial resources are valued at $450000.

**Valuation of the Assets in accordance with the current pricing:**

1. Computers (PC) : 700 \* $750 = $525000
2. Printers: 5 \* $5000 = $25000
3. Model Pool: 20 \* $120 = $2400
4. Routers: 50 \* $80 = $4000
5. DMZ: $30000
6. VPN: $20000

The below table includes the list of assets along with the description and asset value.

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset Number** | **Asset Name** | **Asset Description** | **Asset Value** |
| A1 | Financial Resources | This includes various accounting and audit documents, Payrolls, and applications/tools used for financial calculations. | $450000 |
| A2 | Systems and its components | This includes the physical systems and the components involved in it. |  |
| A2.1 | Computers (PC) | These are the computers that are allocated to employees and owned by HGA. | $525000 |
| A2.2 | Database | This is a private database owned and managed by HGA. Very crucial for the availability of the data. | $600000 |
| A2.3 | Printers | This includes the common printers available among the organization and is responsible for the continuous printing of required documents. | $25000 |
| A2.4 | Hard Disk | A system component that is responsible for storing the data in an individual PC and removable for forensic actions. | $20000 |
| A2.5 | Floppy Disk | Used for data storage purposes. These are movable components of a system that can be used to copy and transfer data. | $5000 |
| A3 | Servers | These are the servers responsible for handling allotted processing among the organization. |  |
| A3.1 | LAN Server | The server which handles Local Area Network operations, Responsible for access and network connections within the organization. | $450000 |
| A3.2 | Email Server | Email servers process the mails and deal with prescribed rules as required by employees. Maintain the communications between the users. | $250000 |
| A4 | Network Related | An asset which is dealing with the network traffic. |  |
| A4.1 | Routers | Used for connection of various devices among the network to the internet. Distributed bandwidth can be achieved. | $4000 |
| A4.2 | WAN | Wide Area Network which is responsible to connect to other Govt agencies. | $300000 |
| A4.3 | VPN Server | Modems are now replaced with VPN server and a VPN application has been provided to employees. | $20000 |
| A5 | Special Administrative Console | A special console is provided to server administrators for administrative and maintenance functions. | $15000 |
| A6 | Personal Information | The personal data of the employees along with phone numbers, passwords, and personal emails. | $330000 |
| A7 | Documents | List of critical documents which are assets of HGA |  |
| A7.1 | Contracting and Procurement Documents | These are multiple documents related to the day-to-day contract and M&A documents | $20000 |
| A7.2 | Internal Correspondence & Draft Regulations | A variety of internal communications and government-associated regulatory documents. | $15000 |
| A8 | Reputation of HGA | An intangible asset of HGA among the government agencies, public, and as well as employees | - |
| A9 | Employee Confidence | Trust and faith build-up for any employee about the organization. | - |
| A10 | DMZ | This is a screened subnet with DMZ. | $30000 |

**Threats to HGA:**

The below table consists of possible threats to HGA.

|  |  |
| --- | --- |
| **Threat Number** | **Threat** |
| T1 | Fraud of Payroll tools/application |
| T2 | Payroll Errors – Manipulated Data |
| T3 | Interruptions of the operations |
| T4 | Cyber Attacks: Ransomware/Malware |
| T5 | Insider Threat |
| T6 | Unauthorized Access |
| T7 | User Accounts Compromised |
| T8 | Brokerage of Information |
| T9 | Natural Disaster |
| T10 | Network Threats |
| T11 | Email Threats |

**Vulnerabilities identified in HGA:**

The below table contains list of vulnerabilities identified among the HGA.

|  |  |
| --- | --- |
| **Vulnerability** | **Vulnerability Description** |
| V1 | Time Sheets Manipulation |
| V2 | Manipulation of Payroll System Entries |
| V3 | Fraudulent employee records |
| V4 | Not following Virus Prevention Analysis |
| V5 | Sensitive Information Disclosure |
| V6 | Unauthorized Access to Sensitive Information |
| V7 | Lack of Authentication mechanisms |
| V8 | Unsecured user Accounts |
| V9 | Lack of Information Security Policies |
| V10 | Contingency Planning errors |
| V11 | Vulnerabilities of Network-Related Attacks |

**Asset and Vulnerability Pair:**

|  |  |  |
| --- | --- | --- |
| **Assets** | | **Vulnerabilities** |
| A1 | Financial Resources | V1: Time Sheets Manipulation |
| V6: Unauthorized Access to Sensitive Information |
| A2 | Systems and its components | V8: Unsecured user Accounts |
| V11: Vulnerabilities of Network-Related Attacks |
| V6: Unauthorized Access to Sensitive Information |
| A3 | Servers | V6: Unauthorized Access to Sensitive Information |
| V8: Unsecured user Accounts |
| V11: Vulnerabilities of Network-Related Attacks |
| A6 | Personal Information | V8: Unsecured user Accounts |
| V1: Time Sheets Manipulation |
| V6: Unauthorized Access to Sensitive Information |

**Threat – Vulnerability matrix:**

The below table consists of the probability of threat and vulnerability among the assets of HGA.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** |
| **V1: Time Sheets Manipulation** | 90 | 95 | 85 | 95 |
| **V6: Unauthorized Access to Sensitive Information** | 95 | 85 | 90 | 80 |
| **V8: Unsecured user Accounts** | 85 | 90 | 80 | 85 |
| **V11: Vulnerabilities of Network-Related Attacks** | 80 | 95 | 90 | 90 |

**Total Threat: 1410**

**Current Security Policies:**

The below table contains the list of current security policies in HGA.

|  |  |  |
| --- | --- | --- |
| **Current Security Control & Policy (CSCP) Number** | **Control & Policy Category** | **Policy Description** |
| CSCP1 | General Use of Computer Systems | Computer Operation Group Responsibilities |
| CSCP2 | General Use of Computer Systems | Security Awareness and Training Pro rams |
| CSCP3 | General use of Computer Systems | Complying with the policies established |
| CSCP4 | General Use of Computer Systems | General Access Control |
| CSCP5 | Payroll Frauds | complying with the Privacy Act |
| CSCP6 | Payroll Frauds | Authorized Access to time and attendance Data |
| CSCP7 | Payroll Frauds | Validation of employee timesheets |
| CSCP8 | Payroll Frauds | Protection against unauthorized execution of timesheet functions |
| CSCP9 | Payroll Frauds | Protection Against Payroll Errors |
| CSCP1O | Payroll Frauds | protection against Accidental Corruption of Data |
| CSCP11 | Interruption of Operations | Contingency Planning by Computer Operations Group |
| CSCP12 | Interruption of Operations | Division Contingency Planning |
| CSCP13 | Information Disclosure | Need to Know the policy |
| CSCP14 | Information Disclosure | Access Control Mechanisms |
| CSCP15 | Information Disclosure | Security Awareness and Training |
| CSCP16 | Network Security | Restricting External Interactions |
| CSCP17 | Network Security | Restrictions on Router |
| CSCP18 | Network Security | LAN restrictions |
| CSCP19 | Non-HGA Systems | External usage policy |

**New Security Policies:**

The below table contains the list of proposed New Security Policies from the Leadership as an outcome of the internal discussions.

|  |  |  |
| --- | --- | --- |
| **New Security Policy** | **Policy Category** | **Policy Description** |
| NSP1 | Payroll Frauds and Vulnerabilities | Stronger Authentication Mechanisms |
| NSP2 |  | Multi-Factor Authentication |
| NSP3 |  | Administrative procedures of systems and servers |
| NSP4 |  | Digital Signatures & Smart Tokens |
| NSP5 | Payroll Errors and Vulnerabilities | Incentives and Penalties for Compliance |
| NSP6 |  | Compliance Audits |
| NSP7 | Continuity of Operations | Security Training and Awareness |
| NSP8 |  | Adherence to Virus prevention procedures |
| NSP9 |  | Automated Backup Program |
| NSP10 | Information Disclosure | Implement compliance audits |
| NSP11 |  | Implementing screen lock policies |
| NSP12 |  | Information storage policy |
| NSP13 |  | Installing activity logs |
| NSP14 | Network related | Strong IAM controls |
| NSP15 |  | Encryption |
| NSP16 |  | Prevention of information disclosure |

**A subset of Assets, Threats, and Vulnerabilities:**

The below 3 tables include the list of the subset of assets. The threats and Vulnerabilities associated with it are considered.

**The subset of Assets:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset Number** | **Asset Name** | **Asset Description** | **Asset Value** |
| A1 | Financial Resources | This includes various accounting and audit documents, Payrolls, and applications/tools used for financial calculations. | $450000 |
| A2 | Systems and it’s components | This includes the physical systems and the components involved in them. | $1,175,000 |
| A3 | Servers | These are the servers responsible for handling allowed processing among the organization. | $700000 |
| A6 | Personal Information | The personal data of the employees along with phone numbers, passwords, and personal emails. | $330000 |

**The subset of Threats:**

|  |  |
| --- | --- |
| **Threat Number** | **Threat** |
| T1 | Fraud of Payroll tools/application |
| T6 | Unauthorized Access |
| T10 | Network Threats |
| T11 | Email Threats |

**The Subset of Vulnerabilities:**

|  |  |
| --- | --- |
| **Vulnerability** | **Vulnerability Description** |
| V1 | Time Sheets Manipulation |
| V6 | Unauthorized Access to Sensitive Information |
| V8 | Unsecured user Accounts |
| V11 | Vulnerabilities of Network-Related Attacks |

**Threat – Vulnerability matrix:**

The below table consists of the probability of threat and vulnerability among the assets of HGA.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** |
| **V1: Time Sheets Manipulation** | 90 | 95 | 85 | 95 |
| **V6: Unauthorized Access to Sensitive Information** | 95 | 85 | 90 | 80 |
| **V8: Unsecured user Accounts** | 85 | 90 | 80 | 85 |
| **V11: Vulnerabilities of Network-Related Attacks** | 80 | 95 | 90 | 90 |

**Total Threat: 1410**

**A brief explanation of the allocated probability values:**

1. Payroll fraud does more impact to any organization because it directly affects the organization's integrity and financial elements. Because the documents used in payroll are very important, there are numerous concerns such as information exposure or theft, unauthorized access, and so on. Accounting, financial audit reports and statements, mergers and acquisitions, and contracts are all part of the organization's secret financial information. A fraudulent timesheet is a vulnerability that must be addressed, and the likelihood of it occurring is very substantial.

2. Unauthorized access to sensitive information is a major concern to the HGA's security posture due to a lack of authentication techniques. The likelihood of information leakage is quite high if a malevolent entity acquires unauthorized access to sensitive information. Information theft and illegal access go hand in hand, which is why the risk of having that vulnerability existing in the system is very high.

3. Unsecured user access occurs because of not safeguarding user accounts which can lead to a data breach. Unsecured accounts will allow attackers to penetrate the system and obtain access to vital assets in several of these scenarios. As a result, the likelihood of encountering those threats is higher.

4. Data protection has become increasingly vital in today's environment, which is why encrypting data is absolutely necessary. The HGA has a LAN Server that links the PCs to the internet and other nodes. As a result, data will be transferred to and from the server as it interacts with various server-side applications, such as e-mail. Unauthorized access and information theft are a possibility if the server's encryption is insufficient.

**Asset and Vulnerability Pair:**

|  |  |  |
| --- | --- | --- |
| **Assets** | | **Vulnerabilities** |
| A1 | Financial Resources | V1: Time Sheets Manipulation |
| V6: Unauthorized Access to Sensitive Information |
| A2 | Systems and its components | V8: Unsecured user Accounts |
| V11: Vulnerabilities of Network-Related Attacks |
| V6: Unauthorized Access to Sensitive Information |
| A3 | Servers | V6: Unauthorized Access to Sensitive Information |
| V8: Unsecured user Accounts |
| V11: Vulnerabilities of Network-Related Attacks |
| A6 | Personal Information | V8: Unsecured user Accounts |
| V1: Time Sheets Manipulation |
| V6: Unauthorized Access to Sensitive Information |

The following is a comparison of present security controls to new leadership's planned controls and policies using the Risk Management Controls model, which includes **Management, Operational, and technical** controls.

|  |  |  |
| --- | --- | --- |
| **Management** | **Operational** | **Technical** |
| Separation of Duties (M1) | Contingency Planning (M5) | Data Loss Prevention techniques (M11) |
| Business Continuity Plans (M2) | Security Training for Employees (M6) | Identity access management controls (M12) |
| Dedicated Incident Response Team (M3) | Security Policy review (M7) | Network traffic monitoring (M13) |
| Compliance Audits (M4) | Data Classification and Backups (M8) | Automated fraudulence payroll detectors (M14) |
|  | Physical Security of Assets (M9) | Threat Intelligence & Reports (M15) |
|  | Security Audits (M10) |  |

**List of current security controls & policies**

|  |  |  |
| --- | --- | --- |
| **Current Security Control & Policy (CSCP) Number** | **Policy Description** | **M-O-T Controls Associated** |
| **General Use of Computer Systems** | | |
| CSCP1 | Computer Operation Group Responsibilities | 1,2,5,8,10 |
| CSCP2 | Security Awareness and Training Programs | 1,2,4,5,6,7,10,14 |
| CSCP3 | Complying with the policies established | 4,5,6,7,8,9,10,11,12,13,14,15 |
| CSCP4 | General Access Control | 5,9,10,12,14 |
| **Payroll Frauds** | | |
| CSCP5 | Complying with the Privacy Act | 2,3,4,5,6,7,9,10,11,12,14 |
| CSCP6 | Authorized Access to time and attendance Data | 4,5,10,12,14 |
| CSCP7 | Validation of employee timesheets | 4,8,10,14 |
| CSCP8 | Protection against unauthorized execution of timesheets | 3,4,8,10,12,14 |
| CSCP9 | Protection against Payroll Errors | 9,11,12,13,14,15 |
| CSCP1O | Protection against Accidental Corruption of Data | 9,11,12,13,14,15 |
| **Interruption of Operations** | | |
| CSCP11 | Contingency Planning by Computer Operations Group | 1,2,4,5,10 |
| CSCP12 | Division Contingency Planning | 1,2,4,5,10 |
| **Information Disclosure** | | |
| CSCP13 | Need to Know the policy | 1,6,10 |
| CSCP14 | Access Control Mechanisms | 4,6,9,10,12 |
| CSCP15 | Security Awareness and Training | 1,4,5,6,10 |
| **Network Security** | | |
| CSCP16 | Restricting External Interactions | 1,4,5,6,9,10,12,13,14 |
| CSCP17 | Restrictions on Router | 3,11,13,14 |
| CSCP18 | LAN restrictions | 3,11,13,14 |
| **Non-HGA Systems** | | |
| CSCP19 | External usage policy | 2,4,5,7,10,12,13,14 |

Chart

Description automatically generated

**List of new security controls & policies:**

|  |  |  |
| --- | --- | --- |
| **New Security Policy** | **Policy Description** | **M-O-T Controls Associated** |
| **Payroll Frauds and Vulnerabilities** | | |
| NSP1 | Stronger Authentication Mechanisms | 4,6,9,10,12 |
| NSP2 | Multi Factor Authentication | 4,6,9,10,12 |
| NSP3 | Administrative procedures of systems and servers | 5,9,10,12,14 |
| NSP4 | Digital Signatures & Smart Tokens | 5,9,10,12,14 |
| **Payroll Errors and Vulnerabilities** | | |
| NSP5 | Incentives and Penalties for Compliance | 1,2,4,5,10 |
| NSP6 | Compliance Audits | 2,3,4,5,6,7,9,10,11,12,14 |
| **Continuity of Operations** | | |
| NSP7 | Security Training and Awareness | 1,2,4,5,6,7,10,14 |
| NSP8 | Adherence to Virus prevention procedures | 9,11,12,13,14,15 |
| NSP9 | Automated Backup Program | 9,11,12,13,14,15 |
| **Information Disclosure** | | |
| NSP10 | Implement compliance audits | 1,4,5,6,9,10,12,13,14 |
| NSP11 | Implementing screen lock policies | 1,4,5,6,9,10,12,13,14 |
| NSP12 | Information storage policy | 9,11,12,13,14,15 |
| NSP13 | Installing activity logs | 1,4,5,6,9,10,12,13,14 |
| **Network related** | | |
| NSP14 | Strong IAM controls | 4,6,9,10,12 |
| NSP15 | Encryption | 3,11,13,14 |
| NSP16 | Prevention of information disclosure | 9,11,12,13,14,15 |

**Security Risk Prevention Strategy Step**

The below calculations reveal the updated Residual Risk Rankings and vulnerability Risk Rankings due to updated threat/vulnerability pairs by implementing M-O-T controls that reduce threat/vulnerability probabilities.

While going through the case study of HGA, there were some security controls that were already implemented by the agency. Although there are some controls that were missing below is the table that outlines the missing controls under the Management — Operational — Technical Categorization. After Implementing these controls, the probability impact reduces significantly.

**Threat vs Vulnerability pairs with Reduced probabilities on Asset Subset — A1, A2, A3, A6 after implementing the above measures.**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** | **T12** |
| **V1: Time Sheets Manipulation** | 25 | 20 | 30 | 15 | 20 |
| **V6: Unauthorized Access to Sensitive Information** | 10 | 25 | 20 | 15 | 35 |
| **V8: Unsecured user Accounts** | 15 | 20 | 10 | 25 | 20 |
| **V11: Vulnerabilities of Network-Related Attacks** | 20 | 15 | 15 | 20 | 10 |
| **V12: VPN application software vulnerabilities** | 15 | 20 | 20 | 15 | 20 |

**Total Threat = 475**

Hence Residual Security Risks – Asset Value \* Threat

**Initial Risk Impact calculation:**

With the considerable zero system resilience and imagining the worst-case scenario with no mitigation or remediation steps applied.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Threat X Vulnerability - Threat Exploiting the Vulnerability** | | | | | | | | | | | | | | | |
| **Assets** | T1 X V1 | T6 X V1 | T10 X V1 | T11 X V1 | T1 X V6 | T6 X V6 | T10 X V6 | T11 X V6 | T1 X V8 | T6 X V8 | T10 X V8 | T11 X V8 | T1 X V11 | T6 X V11 | T10 X V11 | T11 X V11 |
| A1 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| A2 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| A3 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| A6 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |

**Calculation of Residual Asset Security Risks:**

**Calculate Residual Asset Security Risks:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset** | **Asset Value** | **Total Threat** | **Residual Security Risk = (Asset Value \* Total Threat) / 100** |
| A1 | $450,000 | 475 | $2,137,500 |
| A2 | $1,175,000 | 475 | $5,581,250 |
| A3 | $700,000 | 475 | $3,325,000 |
| A6 | $330,000 | 475 | $1,567,500 |
| A4.3 | $20,000 | 475 | $95,000 |
| A10 | $30,000 | 475 | $142,500 |
|  |  |  |  |

**Total Asset Residual Security Risk :** $12,848,750

**Calculate Residual Vulnerability Security Risks:**

1. Risk due to V1 =

[($450,000 \*90) +($1,175,000 \*90)+( $700,000 \*90)+( $330,000 \*90)]/100 = $2389500

1. Risk due to V6 =

[($450,000 \*70) +($1,175,000 \*70)+( $700,000 \*70)+( $330,000 \*70)]/100 = $1858500

1. Risk due to V8 =

[($450,000 \*70) +($1,175,000 \*70)+( $700,000 \*70)+( $330,000 \*70)]/100 = $1858500

1. Risk due to V11 =

[($450,000 \*70) +($1,175,000 \*70)+( $700,000 \*70)+( $330,000 \*70)]/100 = $1858500

1. Risk due to V12 =

[($450,000\*75) +($1,175,000\*75)+($700,000\*75)+($330,000 \*75) +($20,000\*75) +($30,000 \*75)]/100 = $1728750

**Ranking of Security Asset Residual Risks:**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Rank** |
| A2 | $5,581,250 | **1** |
| A3 | $3,325,000 | **2** |
| A1 | $2,137,500 | **3** |
| A6 | $1,567,500 | **4** |
| A10 | $142,500 | **5** |
| A4.3 | $95,000 | **6** |

**Ranking of Vulnerability Security Risks:**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Vulnerability Security Risk** | **Rank** |
| **V1: Time Sheets Manipulation** | $2389500 | **1** |
| **V6: Unauthorized Access to Sensitive Information** | $1858500 | **2** |
| **V8: Unsecured user Accounts** | $1858500 | **3** |
| **V11: Vulnerabilities of Network-Related Attacks** | $1858500 | **4** |
| **V12: VPN application software vulnerabilities** | $1728750 | **5** |

**Security Risk Prevention Strategy P2:**

With the establishment of VPN servers, an employee could be able to connect to the internal network using a VPN application that is installed on the endpoint. This also provides leverage to the cybersecurity team as the traffic monitoring could be achieved and this would help improve the security posture of the company in times of work from home.

When a DMZ is added to the network infrastructure of HGA, DMZ is an important level of network security. DMZ provides an additional layer of security to the network by restricting remote access to internal servers and information, which could be considered as high risk.

**Threat vs Vulnerability pairs with Reduced probabilities on Asset Subset — A1, A2, A3, A6, A10, A4.3 after implementing the M-O-T Controls**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** | **T12** |
| **V1: Time Sheets Manipulation** | 5 | 10 | 5 | 5 | 20 |
| **V6: Unauthorized Access to Sensitive Information** | 10 | 25 | 20 | 15 | 15 |
| **V8: Unsecured user Accounts** | 15 | 20 | 10 | 25 | 20 |
| **V11: Vulnerabilities of Network-Related Attacks** | 20 | 15 | 15 | 20 | 10 |
| **V12: VPN application software vulnerabilities** | 15 | 5 | 20 | 15 | 20 |

**Total Threat = 440**

Hence Residual Security Risks – Asset Value \* Threat

**Initial Risk Impact calculation:**

With the considerable zero system resilience and imagining the worst-case scenario with no mitigation or remediation steps applied.

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Threat X Vulnerability - Threat Exploiting the Vulnerability** | | | | | | | | | | | | | | | |
| **Assets** | T1 X V1 | T6 X V1 | T10 X V1 | T11 X V1 | T1 X V6 | T6 X V6 | T10 X V6 | T11 X V6 | T1 X V8 | T6 X V8 | T10 X V8 | T11 X V8 | T1 X V11 | T6 X V11 | T10 X V11 | T11 X V11 |
| A1 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| A2 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| A3 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| A6 | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% | 100% |
| A4.3 | 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% |

**Calculation of Residual Asset Security Risks:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset** | **Asset Value** | **Total Threat** | **Residual Security Risk = (Asset Value \* Total Threat) / 100** |
| A1 | $450,000 | 375 | $1,687,500 |
| A2 | $1,175,000 | 375 | $4,406,250 |
| A3 | $700,000 | 375 | $2,625,000 |
| A6 | $330,000 | 375 | $1,237,500 |
| A4.3 | $20,000 | 375 | $75,000 |
| A10 | $30,000 | 375 | $112,500 |
|  |  |  |  |

**Total Residual Asset Security Risk = $10,143,750**

**Calculate Residual Vulnerability Security Risks:**

1. Risk due to V1 =

[($450,000\*45) +($1,175,000\*45)+($700,000\*45)+($330,000\*45) +($20,000\*45) +($30,000\*45)]/100 = $1217250

1. Risk due to V6 =

[($450,000\*85) +($1,175,000\*85)+($700,000\*85)+($330,000\*85) +($20,000\*85) +($30,000\*85)]/100 = $2299250

1. Risk due to V8 =

[($450,000\*90) +($1,175,000\*90)+($700,000\*90)+($330,000 \*90) +($20,000\*90) +($30,000 \*90)]/100 = $2434500

1. Risk due to V11 =

[($450,000\*80) +($1,175,000\*80)+($700,000\*80)+( $330,000 \*80) +($20,000\*80) +($30,000 \*80)]/100 = $2164000

1. Risk due to V12 =

[($450,000\*75) +($1,175,000\*75)+($700,000\*75)+($330,000 \*75) +($20,000\*75) +($30,000 \*75)]/100 = $2028750

Total Residual Risk: 370

**Ranking of Security Asset Residual Risks:**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Rank** |
| A2 | $4,406,250 | **1** |
| A3 | $2,625,000 | **2** |
| A1 | $1,687,500 | **3** |
| A6 | $1,237,500 | **4** |
| A10 | $112,500 | **5** |
| A4.3 | $75,000 | **6** |

**Ranking of Vulnerability Security Risks:**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Vulnerability Security Risk** | **Rank** |
| **V8: Unsecured user Accounts** | $2434500 | 1 |
| **V6: Unauthorized Access to Sensitive Information** | $2299250 | 2 |
| **V11: Vulnerabilities of Network-Related Attacks** | $2164000 | 3 |
| **V12: VPN application software vulnerabilities** | $2028750 | 4 |
| **V1: Time Sheets Manipulation** | **$1217250** | **5** |

**Security Risk Prevention Strategy P3:**

According to the above table, **V8: Unsecured user Accounts** is having the highest risk associated according to the Residual Vulnerability Risk ranking. This is considered a critical vulnerability as the attacker may gain access to potentially sensitive information which might be resulting in the leaking of confidential organization strategies and thus impact the operations of the organization.

To overcome this vulnerability, advanced access control techniques must be implemented. Besides, employee training must be done.

Actions to be taken:

1. Passwords safeguarding at workplaces.
2. Shredding of documents must be done before throwing away.
3. Regular employee audits for any information shared outside the organization must be done.
4. Regulations of physical security must be implemented to mitigate internal threats as well as external threats.
5. Regular Monitoring of lateral movements in the organization to detect any potential suspicious activities.
6. NextGen Firewall must be implemented to cut out any inbound traffic.

**Threat vs Vulnerability pairs with Reduced probabilities on Asset Subset — A1, A2, A3, A6, A4.3, A10 after implementing the M-O-T Controls**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** | **T12** |
| **V1: Time Sheets Manipulation** | 5 | 10 | 5 | 5 | 20 |
| **V6: Unauthorized Access to Sensitive Information** | 15 | 20 | 10 | 25 | 20 |
| **V8: Unsecured user Accounts** | 10 | 5 | 5 | 10 | 10 |
| **V11: Vulnerabilities of Network-Related Attacks** | 20 | 15 | 15 | 20 | 10 |
| **V12: VPN application software vulnerabilities** | 15 | 5 | 20 | 15 | 20 |

Hence Residual Security Risks – Asset Value \* Threat

**Calculate Residual Asset Security Risks:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Asset** | **Asset Value** | **Total Threat** | **Residual Security Risk = (Asset Value \* Total Threat) / 100** |
| A1 | $450,000 | 330 | $1,485,000 |
| A2 | $1,175,000 | 330 | $3,877,500 |
| A3 | $700,000 | 330 | $2,310,000 |
| A6 | $330,000 | 330 | $1,089,000 |
| A4.3 | $20,000 | 330 | $66,000 |
| A10 | $30,000 | 330 | $99,000 |
|  |  |  |  |

**Total Residual Risk: $8,926,500**

**Calculate Residual Vulnerability Security Risks:**

1. Risk due to V1 =

[($450,000\*45) +($1,175,000\*45)+($700,000\*45)+($330,000\*45) +($20,000\*45) +($30,000\*45)]/100 = $1217250

1. Risk due to V6 =

[($450,000\*85) +($1,175,000\*85)+($700,000\*85)+($330,000\*85) +($20,000\*85) +($30,000\*85)]/100 = $2299250

1. Risk due to V8 =

**[($450,000\*40) +($1,175,000\*40)+($700,000\*40)+($330,000\*40) +($20,000\*40) +($30,000\*40)]/100 = $1082000**

1. Risk due to V11 =

[($450,000\*80) +($1,175,000\*80)+($700,000\*80)+( $330,000 \*80) +($20,000\*80) +($30,000 \*80)]/100 = $2164000

1. Risk due to V12 =

[($450,000\*75) +($1,175,000\*75)+($700,000\*75)+($330,000 \*75) +($20,000\*75) +($30,000 \*75)]/100 = $2028750

**Ranking of Security Asset Residual Risks:**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Rank** |
| A2 | $3,877,500 | **1** |
| A3 | $2,310,000 | **2** |
| A1 | $1,485,000 | **3** |
| A6 | $1,089,000 | **4** |
| A10 | $99,000 | **5** |
| A4.3 | $66,000 | **6** |

**Ranking of Vulnerability Security Risks:**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Vulnerability Security Risk** | **Rank** |
| **V6: Unauthorized Access to Sensitive Information** | $2299250 | **1** |
| **V11: Vulnerabilities of Network-Related Attacks** | $2164000 | **2** |
| **V12: VPN application software vulnerabilities** | $2028750 | **3** |
| **V1: Time Sheets Manipulation** | $1217250 | **4** |
| **V8: Unsecured user Accounts** | **$1082000** | **5** |

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

According to my observations, VPN and DMZ addition to the HGA network infrastructure is considered as a proactive step taken by the HGA leadership team, However, with the addition of VPN, it comes with additional vulnerabilities and threats where it increases the risk. In the new and old controls of HGA, controls related to VPN were not addressed. As VPN poses a great threat as employees could connect the o internal network from anywhere, extra monitoring of traffic and implementation of firewalls must be taken into consideration. Meanwhile, DMZ is used to mitigate the threats outside the internal network and all the hits on DMZ must be analyzed for any potential suspicious activities and block the IOC’s. DMZ could be used more effectively to mitigate the external threats and regular scanning of the DMZ zone is required to make the environment more secure. Many of the implemented MOT controls also failed to address key issues of security like email safety, antivirus, and firewall on the endpoint. MOT controls mainly focused on the payroll activities and it’s their risks, but a wider perspective of network topology is also a necessity here. As it also has a connection to WAN along with the internet, Lateral movement is possible for an attacker to gain access to HGA if other agencies were compromised. So, the implementation of IAM, Emergency Lockdown and isolation of affected machines must be done. Firewall also plays a crucial role to help mitigate lateral movement. Policies in the network like local perimeter and edge perimeter along with DMZ is considered as a good option as it increases the overall security posture and New or Old MOT controls have failed to address the risks from the above mentioned.

**Security Risk Response (Resilience) Strategy**

**Security Risk Response (Resilience) Strategy Step R1:**

Considering the same Threat Vs Vulnerability pairs as in P3.

In HGA, there are many M-O-T techniques implemented. However, there are a few security tools that still need to be implemented. The Managerial, Operational, and Technical strategies are here considered thus resulting in the reduced impact.

The below table consists of content that is missing in HGA implementations, and these are applied to reduce the probability impact across the HGA.

|  |  |  |
| --- | --- | --- |
| **Management** | **Operational** | **Technical** |
| Separation of Duties | Contingency Planning | Data Loss Prevention techniques |
| Business Continuity Plans | Security Training for Employees | Identity access management controls |
| Dedicated Incident Response Team | Security Policy review | Network traffic monitoring |
| Compliance Audits | Data Classification and Backups | Automated fraudulent payroll detectors |

**Threat vs Vulnerability pairs with Reduced probabilities on Asset Subset — A1, A2, A3, A6 after implementing the M-O-T Controls**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** | **T12** |
| **V1: Time Sheets Manipulation** | 5 | 10 | 5 | 5 | 20 |
| **V6: Unauthorized Access to Sensitive Information** | 5 | 5 | 5 | 5 | 20 |
| **V8: Unsecured user Accounts** | 6 | 9 | 7 | 4 | 10 |
| **V11: Vulnerabilities of Network-Related Attacks** | 7 | 4 | 9 | 8 | 10 |
| **V12: VPN application software vulnerabilities** | 15 | 5 | 20 | 15 | 20 |

**Updated Risk Impact:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Threat X Vulnerability - Threat Exploiting the Vulnerability** | | | | | | | | | | | | | | | |
| **Assets** | **T1 X V1** | **T6 X V1** | **T10 X V1** | **T11 X V1** | **T1 X V6** | **T6 X V6** | **T10 X V6** | **T11 X V6** | **T1 X V8** | **T6 X V8** | **T10 X V8** | **T11 X V8** | **T1 X V11** | **T6 X V11** | **T10 X V11** | **T11 X V11** |
| A1 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| A2 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| A3 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| A6 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| A4.3 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| A10 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **V1 X T12** | **V6 X T12** | **V8 X T12** | **V11 X T12** | **V12 X T12** | **V12 X T1** | **V12 X T6** | **V12 X T 10** | **V12 X T 11** |
| **A1** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| **A2** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| **A3** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| **A6** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| A4.3 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |
| A10 | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** | **50%** |

**Calculate Residual Asset Security Risks:**

***Risk of Asset A1:***

$450,000\*[5\*50+5\*50+6\*50+7\*50+10\*50+5\*50+9\*50+4\*50+5\*50+5\*50+7\*50+9\*50+5\*50+5\*50+4\*50+8\*50+20\*50+20\*50+10\*50+10\*50+20\*50+15\*50+5\*50+20\*50+15\*50] /10000 = $526500

Therefore, partial Asset loss is $526500.

***Risk of Asset A2:*** $1,175,000\*[5\*50+5\*50+6\*50+7\*50+10\*50+5\*50+9\*50+4\*50+5\*50+5\*50+7\*50+9\*50+5\*50+5\*50+4\*50+8\*50+20\*50+20\*50+10\*50+10\*50+20\*50+15\*50+5\*50+20\*50+15\*50] /10000 = $1374750

Therefore, partial Asset loss is $1374750.

***Risk of Asset A3:*** $700,000\*[5\*50+5\*50+6\*50+7\*50+10\*50+5\*50+9\*50+4\*50+5\*50+5\*50+7\*50+9\*50+5\*50+5\*50+4\*50+8\*50+20\*50+20\*50+10\*50+10\*50+20\*50+15\*50+5\*50+20\*50+15\*50] /10000 = $819000

Therefore, partial Asset loss is $819000.

***Risk of Asset A6:*** $330,000\*[5\*50+5\*50+6\*50+7\*50+10\*50+5\*50+9\*50+4\*50+5\*50+5\*50+7\*50+9\*50+5\*50+5\*50+4\*50+8\*50+20\*50+20\*50+10\*50+10\*50+20\*50+15\*50+5\*50+20\*50+15\*50] /10000 = $386100

Therefore, partial Asset loss is $386100.

***Risk of Asset A4.3:***

$20,000\*[5\*50+5\*50+6\*50+7\*50+10\*50+5\*50+9\*50+4\*50+5\*50+5\*50+7\*50+9\*50+5\*50+5\*50+4\*50+8\*50+20\*50+20\*50+10\*50+10\*50+20\*50+15\*50+5\*50+20\*50+15\*50] /10000 = $23400

Therefore, partial Asset loss is $23400.

***Risk of Asset A10:***

$30,000\*[5\*50+5\*50+6\*50+7\*50+10\*50+5\*50+9\*50+4\*50+5\*50+5\*50+7\*50+9\*50+5\*50+5\*50+4\*50+8\*50+20\*50+20\*50+10\*50+10\*50+20\*50+15\*50+5\*50+20\*50+15\*50] /10000 = $35100

Therefore, partial Asset loss is $35100.

**Calculate Residual Vulnerability Security Risks:**

***Risk due to V1:*** $450,000\*[5\*50+10\*50+5\*50+5\*50+20\*50]+ $1,175,000\*[5\*50+10\*50+5\*50+5\*50+20\*50]+ $700,000\*[5\*50+10\*50+5\*50+5\*50+20\*50]+ $330,000\*[5\*50+10\*50+5\*50+5\*50+20\*50]+ $20,000\*[5\*50+10\*50+5\*50+5\*50+20\*50]+ $30,000\*[5\*50+10\*50+5\*50+5\*50+20\*50]/10000 = $608625

***Risk due to V6:*** $450,000\*[5\*50+5\*50+5\*50+5\*50+20\*50]+ $1,175,000\*[5\*50+5\*50+5\*50+5\*50+20\*50]+ $700,000\*[5\*50+5\*50+5\*50+5\*50+20\*50]+ $330,000\*[5\*50+5\*50+5\*50+5\*50+20\*50] + $20,000\*[5\*50+5\*50+5\*50+5\*50+20\*50]+ $30,000\*[5\*50+5\*50+5\*50+5\*50+20\*50]/10000 = $541000

***Risk due to V8:*** $450,000\*[6\*50+9\*50+7\*50+4\*50+10\*50]+ $1,175,000\*[6\*50+9\*50+7\*50+4\*50+10\*50]+ $700,000\*[6\*50+9\*50+7\*50+4\*50+10\*50]+ $330,000\*[6\*50+9\*50+7\*50+4\*50+10\*50] + $20,000\*[6\*50+9\*50+7\*50+4\*50+10\*50]+ $30,000\*[6\*50+9\*50+7\*50+4\*50+10\*50]/10000 = $486900

***Risk due to V11:*** $450,000\*[7\*50+4\*50+9\*50+8\*50+10\*50]+ $1,175,000\*[7\*50+4\*50+9\*50+8\*50+10\*50]+ $700,000\*[7\*50+4\*50+9\*50+8\*50+10\*50]+ $330,000\*[7\*50+4\*50+9\*50+8\*50+10\*50] + $20,000\*[7\*50+4\*50+9\*50+8\*50+10\*50]+ $30,000\*[7\*50+4\*50+9\*50+8\*50+10\*50]/10000 = $513950

***Risk due to V12:*** $450,000\*[15\*50+5\*50+20\*50+15\*50+29\*50]+ $1,175,000\*[15\*50+5\*50+20\*50+15\*50+29\*50]+ $700,000\*[15\*50+5\*50+20\*50+15\*50+29\*50]+ $330,000\*[15\*50+5\*50+20\*50+15\*50+29\*50] + $20,000\*[15\*50+5\*50+20\*50+15\*50+29\*50]+ $30,000\*[15\*50+5\*50+20\*50+15\*50+29\*50]/10000 = $1123501

**Ranking of Security Asset Residual Risks:**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Rank** |
| A2 | $1,374,750 | **1** |
| A3 | $819,000 | **2** |
| A1 | $526,500 | **3** |
| A6 | $386,100 | **4** |
| A10 | $35,100 | **5** |
| A4.3 | $23,400 | **6** |

**Ranking of Vulnerability Security Risks:**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Vulnerability Security Risk** | **Rank** |
| **V12: VPN application software vulnerabilities** | $1,123,501 | **1** |
| **V1: Time Sheets Manipulation** | $608,625 | **2** |
| **V6: Unauthorized Access to Sensitive Information** | $541,000 | **3** |
| **V11: Vulnerabilities of Network-Related Attacks** | $513,950 | **4** |
| **V8: Unsecured user Accounts** | $486,900 | **5** |

**Security Risk Response (Resilience) Strategy Step R2:**

Additional Risk reduction controls such as blocking suspicious activities or adding a firewall were applied to the highest-ranked Residual Asset Risk, further reducing risk effect probability, the overall security asset residual risk, and establishing a new vulnerability security risk ranking.

From the Security Asset Residual Risk Ranking Table of R1, the highest-ranked Asset is **A2: Systems and it’s components**. Configuring the systems with more End-Point security tools and logs monitoring might reduce the overall risk. Also, advanced authentication mechanisms and firewalls along with AV installed on systems can reduce the impact.

**Threat vs Vulnerability pairs with Reduced probabilities on Asset Subset — A1, A2, A3, A6 after implementing the M-O-T Controls**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** | **T12** |
| **V1: Time Sheets Manipulation** | 5 | 10 | 5 | 5 | 20 |
| **V6: Unauthorized Access to Sensitive Information** | 5 | 5 | 5 | 5 | 20 |
| **V8: Unsecured user Accounts** | 6 | 9 | 7 | 4 | 10 |
| **V11: Vulnerabilities of Network-Related Attacks** | 7 | 4 | 9 | 8 | 10 |
| **V12: VPN application software vulnerabilities** | 15 | 5 | 20 | 15 | 20 |

**Updated Risk Impact:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Threat X Vulnerability - Threat Exploiting the Vulnerability** | | | | | | | | | | | | | | | |
| **Assets** | T1 X V1 | T6 X V1 | T10 X V1 | T11 X V1 | T1 X V6 | T6 X V6 | T10 X V6 | T11 X V6 | T1 X V8 | T6 X V8 | T10 X V8 | T11 X V8 | T1 X V11 | T6 X V11 | T10 X V11 | T11 X V11 |
| A1 | **50%** | 30% | 50% | 40% | **50%** | 30% | 50% | 40% | **50%** | 30% | 50% | 20% | **30%** | 40% | 50% | 40% |
| **A2** | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **10%** | **5%** |
| A3 | **50%** | 20% | 50% | 50% | **20%** | 50% | 30% | 20% | **50%** | 50% | 40% | 50% | **40%** | 50% | 20% | 30% |
| A6 | **30%** | 40% | 50% | 20% | **30%** | 40% | 20% | 50% | **20%** | 40% | 30% | 40% | **50%** | 50% | 30% | 50% |
| A10 | **30%** | 40% | 50% | 20% | **30%** | 40% | 20% | 50% | **20%** | 40% | 30% | 40% | **50%** | 50% | 30% | 50% |
| A4.3 | **30%** | 40% | 50% | 20% | **30%** | 40% | 20% | 50% | **20%** | 40% | 30% | 40% | **50%** | 50% | 30% | 50% |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **V1 X T12** | **V6 X T12** | **V8 X T12** | **V11 X T12** | **V12 X T12** | **V12 X T1** | **V12 X T6** | **V12 X T 10** | **V12 X T 11** |
| **A1** | 50% | 30% | 50% | 40% | 50% | 30% | 50% | 40% | 50% |
| **A2** | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** |
| A3 | 50% | 20% | 50% | 50% | 20% | 50% | 30% | 20% | 50% |
| A6 | 50% | 50% | 50% | 50% | 50% | 50% | 50% | 50% | 50% |
| A10 | 30% | 40% | 50% | 20% | 30% | 40% | 20% | 50% | 20% |  |
| A4.3 | 30% | 40% | 50% | 20% | 30% | 40% | 20% | 50% | 20% |  |

**Calculate Residual Asset Security Risks:**

***Risk of Asset A1:***

$450,000\*[5\*50+5\*50+6\*50+7\*30+10\*30+5\*30+9\*30+4\*40+5\*50+5\*50+7\*50+9\*50+5\*40+5\*40+4\*20+8\*40+20\*50+20\*30+10\*50+10\*40+20\*50+15\*30+5\*50+20\*40+15\*50] /10000 = $438300

Therefore, partial Asset loss is $438300.

***Risk of Asset A2:*** $1,175,000\*[5\*5+5\*15+6\*5+7\*10+10\*10+5\*15+9\*10+4\*5+5\*15+5\*10+7\*10+9\*5+5\*10+5\*15+4\*10+8\*15+20\*10+20\*5+10\*15+10\*10+20\*5+15\*15+5\*10+20\*10+15\*5] /10000 = $259675

Therefore, partial Asset loss is $259675.

***Risk of Asset A3:*** $700,000\*[5\*50+5\*20+6\*50+7\*40+10\*20+5\*50+9\*50+4\*50+5\*50+5\*20+7\*50+9\*20+5\*30+5\*30+4\*20+8\*50+20\*50+20\*20+10\*30+10\*50+20\*40+15\*30+5\*20+20\*40+15\*50] /10000 = $615300

Therefore, partial Asset loss is $615300.

***Risk of Asset A6:*** $330,000\*[5\*40+5\*50+6\*30+7\*20+10\*50+5\*50+9\*30+4\*30+5\*50+5\*40+7\*50+9\*30+5\*20+5\*40+4\*50+8\*50+20\*50+20\*30+10\*50+10\*40+20\*50+15\*20+5\*30+20\*40+15\*50] /10000 = $309540

Therefore, partial Asset loss is $309540.

***Risk of Asset A4.3:***

$20,000\*[5\*30+5\*50+6\*40+7\*50+10\*50+5\*20+9\*50+4\*50+5\*30+5\*50+7\*40+9\*50+5\*50+5\*40+4\*40+8\*50+20\*30+20\*50+10\*20+10\*50+20\*20+15\*20+5\*50+20\*40+15\*50] /10000 = $18360

Therefore, partial Asset loss is $18360.

***Risk of Asset A10:***

$30,000\*[5\*30+5\*20+6\*30+7\*50+10\*50+5\*40+9\*50+4\*20+5\*50+5\*30+7\*50+9\*40+5\*50+5\*40+4\*50+8\*50+20\*30+20\*50+10\*20+10\*50+20\*30+15\*40+5\*50+20\*40+15\*50] /10000 = $28410

Therefore, partial Asset loss is $28410.

**Calculate Residual Vulnerability Security Risks:**

***Risk due to V1:*** $450,000\*[5\*50+10\*30+5\*40+5\*50+20\*20]+ $1,175,000\*[5\*10+10\*10+5\*5+5\*15+20\*5]+ $700,000\*[5\*30+10\*50+5\*20+5\*40+20\*50]+ $330,000\*[5\*30+10\*50+5\*30+5\*50+20\*40]+ $20,000\*[5\*30+10\*40+5\*30+5\*40+20\*50]+ $30,000\*[5\*40+10\*50+5\*30+5\*20+20\*40]/10000 = $310725

***Risk due to V6:*** $450,000\*[5\*30+5\*50+5\*40+5\*50+20\*40]+ $1,175,000\*[5\*10+5\*5+5\*10+5\*15+20\*20]+ $700,000\*[5\*50+5\*40+5\*30+5\*20+20\*20]+ $330,000\*[5\*30+5\*40+5\*50+5\*40+20\*50] + $20,000\*[5\*40+5\*50+5\*30+5\*50+20\*20]+ $30,000\*[5\*20+5\*50+5\*40+5\*30+20\*20]/10000 = $286950

***Risk due to V8:*** $450,000\*[6\*50+9\*20+7\*20+4\*50+10\*40]+ $1,175,000\*[6\*10+9\*5+7\*15+4\*15+10\*10]+ $700,000\*[6\*50+9\*40+7\*40+4\*20+10\*30]+ $330,000\*[6\*40+9\*40+7\*30+4\*50+10\*50] + $20,000\*[6\*20+9\*50+7\*30+4\*50+10\*40]+ $30,000\*[6\*20+9\*30+7\*50+4\*50+10\*40]/10000 = $247385

***Risk due to V11:*** $450,000\*[7\*50+4\*30+9\*40+8\*50+10\*20]+ $1,175,000\*[7\*5+4\*5+9\*15+8\*10+10\*15]+ $700,000\*[7\*40+4\*50+9\*50+8\*30+10\*20]+ $330,000\*[7\*20+4\*50+9\*40+8\*50+10\*30] + $20,000\*[7\*50+4\*30+9\*40+8\*50+10\*30]+ $30,000\*[7\*30+4\*50+9\*50+8\*40+10\*50]/10000 = $263900

***Risk due to V12:*** $450,000\*[15\*40+5\*30+20\*40+15\*40+29\*30]+ $1,175,000\*[15\*10+5\*15+20\*5+15\*5+29\*10]+ $700,000\*[15\*40+5\*50+20\*50+15\*30+29\*20]+ $330,000\*[15\*50+5\*50+20\*30+15\*50+29\*50] + $20,000\*[15\*50+5\*20+20\*50+15\*40+29\*30]+ $30,000\*[15\*30+5\*50+20\*40+15\*50+29\*30]/10000 = $559975

**Ranking of Security Asset Residual Risks:**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Rank** |
| A3 | $615,300 | **1** |
| A1 | $438,300 | **2** |
| A6 | $309,540 | **3** |
| A2 | $259,675 | **4** |
| A10 | $28,410 | **5** |
| A4.3 | $18,360 | **6** |

**Ranking of Vulnerability Security Risks:**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Vulnerability Security Risk** | **Rank** |
| **V12: VPN application software vulnerabilities** | $559975 | **1** |
| **V1: Time Sheets Manipulation** | $310725 | **2** |
| **V6: Unauthorized Access to Sensitive Information** | $286950 | **3** |
| **V11: Vulnerabilities of Network-Related Attacks** | $263900 | **4** |
| **V8: Unsecured user Accounts** | $247385 | **5** |

**Security Risk Response (Resilience) Strategy Step R3:**

Additional Risk reduction controls such as blocking suspicious activities or adding a firewall were applied to the highest-ranked Residual Asset Risk, further reducing risk effect probability, the overall security asset residual risk, and establishing a new vulnerability security risk ranking.

From the Security Asset Residual Risk Ranking Table of R2, the highest-ranked Asset is **A3: Servers.** Servers are crucial for any organization. To protect the servers, additional security measures like the authenticity of individual access to the financial data must be verified. Configuring the systems with more End-Point security tools and logs monitoring might reduce the overall risk. Also, advanced authentication mechanisms and firewalls along with AV installed on systems can reduce the impact.

**Threat vs Vulnerability pairs with Reduced probabilities on Asset Subset — A1, A2, A3, A6 after implementing the M-O-T Controls**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** | **T12** |
| **V1: Time Sheets Manipulation** | 5 | 10 | 5 | 5 | 20 |
| **V6: Unauthorized Access to Sensitive Information** | 5 | 5 | 5 | 5 | 20 |
| **V8: Unsecured user Accounts** | 6 | 9 | 7 | 4 | 10 |
| **V11: Vulnerabilities of Network-Related Attacks** | 7 | 4 | 9 | 8 | 10 |
| **V12: VPN application software vulnerabilities** | 15 | 5 | 20 | 15 | 20 |

**Updated Risk Impact:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Threat X Vulnerability - Threat Exploiting the Vulnerability** | | | | | | | | | | | | | | | |
| **Assets** | T1 X V1 | T6 X V1 | T10 X V1 | T11 X V1 | T1 X V6 | T6 X V6 | T10 X V6 | T11 X V6 | T1 X V8 | T6 X V8 | T10 X V8 | T11 X V8 | T1 X V11 | T6 X V11 | T10 X V11 | T11 X V11 |
| A1 | **50%** | 30% | 50% | 40% | **50%** | 30% | 50% | 40% | **50%** | 30% | 50% | 20% | **30%** | 40% | 50% | 40% |
| **A2** | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **10%** | **5%** |
| A3 | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **10%** | **5%** |
| A6 | **30%** | 40% | 50% | 20% | **30%** | 40% | 20% | 50% | **20%** | 40% | 30% | 40% | **50%** | 50% | 30% | 50% |
| A10 | **30%** | 40% | 50% | 20% | **30%** | 40% | 20% | 50% | **20%** | 40% | 30% | 40% | **50%** | 50% | 30% | 50% |
| A4.3 | **30%** | 40% | 50% | 20% | **30%** | 40% | 20% | 50% | **20%** | 40% | 30% | 40% | **50%** | 50% | 30% | 50% |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **V1 X T12** | **V6 X T12** | **V8 X T12** | **V11 X T12** | **V12 X T12** | **V12 X T1** | **V12 X T6** | **V12 X T 10** | **V12 X T 11** |
| **A1** | 50% | 20% | 50% | 50% | 20% | 50% | 30% | 20% | 50% |
| **A2** | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** |
| A3 | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** |
| A6 | 50% | 50% | 50% | 50% | 50% | 50% | 50% | 50% | 50% |
| A10 | 30% | 40% | 50% | 20% | 30% | 40% | 20% | 50% | 20% |  |
| A4.3 | 30% | 40% | 50% | 20% | 30% | 40% | 20% | 50% | 20% |  |

**Calculate Residual Asset Security Risks:**

***Risk of Asset A1:***

$450,000\*[5\*50+5\*50+6\*50+7\*30+10\*30+5\*30+9\*30+4\*40+5\*50+5\*50+7\*50+9\*50+5\*40+5\*40+4\*20+8\*40+20\*50+20\*30+10\*50+10\*40+20\*50+15\*30+5\*50+20\*40+15\*50] /10000 = $438300

Therefore, partial Asset loss is $438300.

***Risk of Asset A2:*** $1,175,000\*[5\*5+5\*15+6\*5+7\*10+10\*10+5\*15+9\*10+4\*5+5\*15+5\*10+7\*10+9\*5+5\*10+5\*15+4\*10+8\*15+20\*10+20\*5+10\*15+10\*10+20\*5+15\*15+5\*10+20\*10+15\*5] /10000 = $259675

Therefore, partial Asset loss is $259675.

***Risk of Asset A3:*** $700,000\*[5\*5+5\*15+6\*5+7\*10+10\*15+5\*5+9\*10+4\*10+5\*5+5\*15+7\*10+9\*5+5\*10+5\*10+4\*10+8\*15+20\*10+20\*5+10\*5+10\*10+20\*10+15\*10+5\*15+20\*10+15\*15] /10000 = $102600

Therefore, partial Asset loss is $102600.

***Risk of Asset A6:*** $330,000\*[5\*40+5\*50+6\*30+7\*20+10\*50+5\*50+9\*30+4\*30+5\*50+5\*40+7\*50+9\*30+5\*20+5\*40+4\*50+8\*50+20\*50+20\*30+10\*50+10\*40+20\*50+15\*20+5\*30+20\*40+15\*50] /10000 = $309540

Therefore, partial Asset loss is $309540.

***Risk of Asset A4.3:***

$20,000\*[5\*30+5\*50+6\*40+7\*50+10\*50+5\*20+9\*50+4\*50+5\*30+5\*50+7\*40+9\*50+5\*50+5\*40+4\*40+8\*50+20\*30+20\*50+10\*20+10\*50+20\*20+15\*20+5\*50+20\*40+15\*50] /10000 = $18360

Therefore, partial Asset loss is $18360.

***Risk of Asset A10:***

$30,000\*[5\*30+5\*20+6\*30+7\*50+10\*50+5\*40+9\*50+4\*20+5\*50+5\*30+7\*50+9\*40+5\*50+5\*40+4\*50+8\*50+20\*30+20\*50+10\*20+10\*50+20\*30+15\*40+5\*50+20\*40+15\*50] /10000 = $28410

Therefore, partial Asset loss is $28410.

**Calculate Residual Vulnerability Security Risks:**

***Risk due to V1:*** $450,000\*[5\*50+10\*30+5\*40+5\*50+20\*20]+ $1,175,000\*[5\*10+10\*10+5\*5+5\*15+20\*5]+ $700,000\*[5\*10+10\*10+5\*5+5\*10+20\*15]+ $330,000\*[5\*30+10\*50+5\*30+5\*50+20\*40]+ $20,000\*[5\*30+10\*40+5\*30+5\*40+20\*50]+ $30,000\*[5\*40+10\*50+5\*30+5\*20+20\*40]/10000 = $210975

***Risk due to V6:*** $450,000\*[5\*30+5\*50+5\*40+5\*50+20\*40]+ $1,175,000\*[5\*10+5\*5+5\*10+5\*15+20\*20]+ $700,000\*[5\*10+5\*5+5\*20+5\*5+20\*15]+ $330,000\*[5\*30+5\*40+5\*50+5\*40+20\*50] + $20,000\*[5\*40+5\*50+5\*30+5\*50+20\*20]+ $30,000\*[5\*20+5\*50+5\*40+5\*30+20\*20]/10000 = $244950

***Risk due to V8:*** $450,000\*[6\*50+9\*20+7\*20+4\*50+10\*40]+ $1,175,000\*[6\*10+9\*5+7\*15+4\*15+10\*10]+ $700,000\*[6\*10+9\*10+7\*5+4\*15+10\*10]+ $330,000\*[6\*40+9\*40+7\*30+4\*50+10\*50] + $20,000\*[6\*20+9\*50+7\*30+4\*50+10\*40]+ $30,000\*[6\*20+9\*30+7\*50+4\*50+10\*40]/10000 = $179135

***Risk due to V11:*** $450,000\*[7\*50+4\*30+9\*40+8\*50+10\*20]+ $1,175,000\*[7\*5+4\*5+9\*15+8\*10+10\*15]+ $700,000\*[7\*10+4\*5+9\*10+8\*15+10\*10]+ $330,000\*[7\*20+4\*50+9\*40+8\*50+10\*30] + $20,000\*[7\*50+4\*30+9\*40+8\*50+10\*30]+ $30,000\*[7\*30+4\*50+9\*50+8\*40+10\*50]/10000 = $196000

***Risk due to V12:*** $450,000\*[15\*40+5\*30+20\*40+15\*40+29\*30]+ $1,175,000\*[15\*10+5\*15+20\*5+15\*5+29\*10]+ $700,000\*[15\*10+5\*5+20\*15+15\*10+29\*15]+ $330,000\*[15\*50+5\*50+20\*30+15\*50+29\*50] + $20,000\*[15\*50+5\*20+20\*50+15\*40+29\*30]+ $30,000\*[15\*30+5\*50+20\*40+15\*50+29\*30]/10000 = $432575

**Ranking of Security Asset Residual Risks:**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Rank** |
| A1 | $438,300 | **1** |
| A6 | $309,540 | **2** |
| A2 | $259,675 | **3** |
| A3 | $102,600 | **4** |
| A10 | $28,410 | **5** |
| A4.3 | $18,360 | **6** |

**Ranking of Vulnerability Security Risks:**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Vulnerability Security Risk** | **Rank** |
| **V12: VPN application software vulnerabilities** | $432575 | **1** |
| **V6: Unauthorized Access to Sensitive Information** | $244950 | **2** |
| **V1: Time Sheets Manipulation** | $210975 | **3** |
| **V11: Vulnerabilities of Network-Related Attacks** | $196000 | **4** |
| **V8: Unsecured user Accounts** | $179135 | **5** |

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

According to my observations, VPN and DMZ addition to the HGA network infrastructure is considered as a proactive step taken by the HGA leadership team, However, with the addition of VPN, it comes with additional vulnerabilities and threats where it increases the risk. In the new and old controls of HGA, controls related to VPN were not addressed. As VPN poses a great threat as employees could connect the o internal network from anywhere, extra monitoring of traffic and implementation of firewalls must be taken into consideration. Meanwhile, DMZ is used to mitigate the threats outside the internal network and all the hits on DMZ must be analyzed for any potential suspicious activities and block the IOC’s. DMZ could be used more effectively to mitigate the external threats and regular scanning of the DMZ zone is required to make the environment more secure. Many of the implemented MOT controls also failed to address key issues of security like email safety, antivirus, and firewall on the endpoint. MOT controls mainly focused on the payroll activities and it’s their risks, but a wider perspective of network topology is also a necessity here. As it also has a connection to WAN along with the internet, Lateral movement is possible for an attacker to gain access to HGA if other agencies were compromised. So, the implementation of IAM, Emergency Lockdown, and isolation of affected machines must be done. The firewall also plays a crucial role to help mitigate lateral movement. Policies in the network like local perimeter and edge perimeter along with DMZ is considered as a good option as it increases the overall security posture and New or Old MOT controls have failed to address the risks from the above mentioned.

**Mixed Strategy:**

**Security Risk Response (Resilience) Strategy & Security Risk Prevention Strategy**

Combining the strategies implemented in S3 and R3, along with new policies proposed by leadership are being included in the below calculations.

The probabilities are greatly lowered by incorporating new preventive and responsive security procedures. Unauthorized disclosure of information will be prevented by preventive controls such as encrypting the database for confidentiality and hashing the contents for integrity. A disaster recovery plan can be a responsive strategy for recovering from any events. The threat vulnerability pairs matrix and Risk Impact table have been revised with reduced probabilities.

**Threat vs Vulnerability pairs with Reduced probabilities on Asset Subset — A1, A2, A3, A6 after implementing the M-O-T Controls**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **T1** | **T6** | **T10** | **T11** | **T12** |
| **V1: Time Sheets Manipulation** | 5 | 10 | 5 | 5 | 5 |
| **V6: Unauthorized Access to Sensitive Information** | 5 | 5 | 5 | 5 | 3 |
| **V8: Unsecured user Accounts** | 6 | 9 | 7 | 4 | 2 |
| **V11: Vulnerabilities of Network-Related Attacks** | 7 | 4 | 9 | 8 | 5 |
| **V12: VPN application software vulnerabilities** | 2 | 5 | 3 | 4 | 6 |

**Updated Risk Impact:**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | **Threat X Vulnerability - Threat Exploiting the Vulnerability** | | | | | | | | | | | | | | | |
| **Assets** | T1 X V1 | T6 X V1 | T10 X V1 | T11 X V1 | T1 X V6 | T6 X V6 | T10 X V6 | T11 X V6 | T1 X V8 | T6 X V8 | T10 X V8 | T11 X V8 | T1 X V11 | T6 X V11 | T10 X V11 | T11 X V11 |
| A1 | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **50%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** |
| **A2** | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **10%** | **5%** |
| A3 | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **10%** | **5%** |
| A6 | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **5%** | **15%** |
| A10 | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **5%** | **15%** | **10%** |
| A4.3 | **10%** | **5%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **5%** | **15%** |

|  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **V1 X T12** | **V6 X T12** | **V8 X T12** | **V11 X T12** | **V12 X T12** | **V12 X T1** | **V12 X T6** | **V12 X T 10** | **V12 X T 11** |
| **A1** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **5%** | **15%** |
| **A2** | **10%** | **5%** | **10%** | **5%** | **5%** | **10%** | **5%** | **10%** | **5%** |
| A3 | **10%** | **5%** | **10%** | **5%** | **10%** | **10%** | **5%** | **10%** | **5%** |
| A6 | **5%** | **10%** | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** |
| A10 | **5%** | **10%** | **5%** | **15%** | **5%** | **5%** | **10%** | **5%** | **15%** |  |
| A4.3 | **5%** | **15%** | **10%** | **5%** | **10%** | **5%** | **15%** | **5%** | **15%** |  |

**Calculate Residual Asset Security Risks:**

***Risk of Asset A1:***

$450,000\*[5\*10+5\*5+6\*15+7\*10+10\*10+5\*5+9\*15+4\*10+5\*5+5\*10+7\*15+9\*5+5\*10+5\*5+4\*5+8\*10+4\*15+9\*10+6\*15+4\*10+5\*10+6\*15+5\*15+9\*10+5\*10] /10000 = $70650

Therefore, partial Asset loss is $70650.

***Risk of Asset A2:*** $1,175,000\*[5\*15+5\*5+2\*10+6\*10+4\*10+3\*10+7\*5+4\*5+5\*5+5\*5+6\*5+5\*10+3\*10+4\*5+4\*15+6\*5+20\*10+20\*5+10\*15+10\*10+20\*5+15\*15+5\*10+20\*10+15\*5] /10000 = $208562

Therefore, partial Asset loss is $208562.

***Risk of Asset A3:*** $700,000\*[5\*5+5\*15+2\*5+6\*10+4\*10+3\*10+7\*15+4\*5+5\*5+5\*5+6\*10+5\*10+3\*5+4\*10+4\*5+6\*5+2\*10+3\*5+5\*5+5\*10+6\*10+8\*10+9\*15+6\*10+5\*15] /10000 = $80500

Therefore, partial Asset loss is $80500.

***Risk of Asset A6:*** $330,000\*[5\*10+5\*10+6\*15+7\*10+10\*5+5\*5+9\*10+4\*10+5\*5+5\*15+7\*5+9\*15+5\*10+5\*10+4\*5+8\*5+2\*10+3\*15+8\*10+6\*15+5\*5+5\*10+5\*10+4\*15+9\*5] /10000 = $44880

Therefore, partial Asset loss is $.

***Risk of Asset A4.3:***

$20,000\*[5\*10+5\*10+6\*15+7\*10+10\*5+5\*5+9\*10+4\*10+5\*5+5\*15+7\*5+9\*15+5\*10+5\*10+4\*5+8\*15+2\*10+3\*5+8\*10+6\*15+5\*15+6\*5+5\*10+5\*10+9\*15] /10000 = $3040

Therefore, partial Asset loss is $.

***Risk of Asset A10:***

$30,000\*[5\*10+5\*10+6\*15+7\*10+10\*5+5\*5+9\*10+4\*10+5\*5+5\*15+7\*5+9\*15+5\*10+5\*10+4\*5+8\*5+2\*10+3\*5+9\*10+6\*10+8\*5+5\*10+6\*10+4\*15+6\*5] /10000 = $3960

Therefore, partial Asset loss is $.

**Calculate Residual Vulnerability Security Risks:**

***Risk due to V1:*** $450,000\*[5\*5+6\*15+8\*5+5\*10+2\*15]+ $1,175,000\*[5\*10+10\*10+5\*5+5\*15+20\*5]+ $700,000\*[5\*5+6\*15+8\*5+5\*10+2\*15]+ $330,000\*[5\*5+6\*15+8\*5+5\*10+2\*15]+ $20,000\*[5\*5+6\*15+8\*5+5\*10+2\*15]+ $30,000\*[5\*5+6\*15+8\*5+5\*10+2\*15]/10000 = $77080

***Risk due to V6:*** $450,000\*[5\*10+5\*5+5\*15+5\*10+6\*5]+ $1,175,000\*[5\*10+5\*5+5\*15+5\*10+6\*50]+ $700,000\*[5\*10+5\*5+5\*15+5\*10+6\*5]+ $330,000\*[5\*10+5\*5+5\*15+5\*10+6\*5] + $20,000\*[5\*10+5\*5+5\*15+5\*10+6\*5]+ $30,000\*[5\*10+5\*5+5\*15+5\*10+6\*5]/10000 = $93940

***Risk due to V8:*** $450,000\*[6\*10+9\*15+7\*5+4\*5+10\*10]+ $1,175,000\*[6\*10+9\*15+7\*5+4\*5+10\*10]+ $700,000\*[6\*10+9\*15+7\*5+4\*5+10\*10]+ $330,000\*[6\*10+9\*15+7\*5+4\*5+10\*10] + $20,000\*[6\*10+9\*15+7\*5+4\*5+10\*10]+ $30,000\*[6\*10+9\*15+7\*5+4\*5+10\*10]/10000 = $94675

***Risk due to V11:*** $450,000\*[7\*10+4\*15+9\*10+8\*5+10\*10]+ $1,175,000\*[7\*5+4\*5+9\*15+8\*10+10\*15]+ $700,000\*[7\*10+4\*15+9\*10+8\*5+10\*10]+ $330,000\*[7\*10+4\*15+9\*10+8\*5+10\*10] + $20,000\*[7\*10+4\*15+9\*10+8\*5+10\*10]+ $30,000\*[7\*10+4\*15+9\*10+8\*5+10\*10]/10000 = $104430

***Risk due to V12:*** $450,000\*[5\*10+6\*15+8\*10+9\*15+6\*10]+ $1,175,000\*[5\*10+6\*15+8\*10+9\*15+6\*10]+ $700,000\*[5\*10+6\*15+8\*10+9\*15+6\*10]+ $330,000\*[5\*10+6\*15+8\*10+9\*15+6\*10] + $20,000\*[5\*10+6\*15+8\*10+9\*15+6\*10]+ $30,000\*[5\*10+6\*15+8\*10+9\*15+6\*10]/10000 = $112257

**Ranking of Security Asset Residual Risks:**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Rank** |
| A2 | $208,562 | **1** |
| A3 | $80,500 | **2** |
| A1 | $70,650 | **3** |
| A6 | $44,880 | **4** |
| A10 | $3,960 | **5** |
| A4.3 | $3,040 | **6** |

**Ranking of Vulnerability Security Risks:**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Vulnerability Security Risk** | **Rank** |
| **V12: VPN application software vulnerabilities** | $112,257 | **1** |
| **V11: Vulnerabilities of Network-Related Attacks** | $104,430 | **2** |
| **V8: Unsecured user Accounts** | $94,675 | **3** |
| **V6: Unauthorized Access to Sensitive Information** | $93,940 | **4** |
| **V1: Time Sheets Manipulation** | $77,080 | **5** |

**Conclusion: Cost-Benefit Analysis**

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

I believe that HGA has addressed most of the critical security risks and the new controls proposed by the new CISO and team are covering most of them. However, I feel like there are many other controls that could be considered.

Only the Incident Response team is considered in HGA, but there must be other teams such as Red Team which works on the offensive side to identify more vulnerabilities thus providing more chance of assessing the accurate risk when seen from an attacker’s perspective.

The addition of many new tools and software and processes must be taken into consideration to protect endpoints, new software and mitigate the third part risks as well. I believe still there is room to grow for HGA and the new CISO team to concentrate in these areas. Phishing is a great threat to any organization and perfect controls to defend against phishing attacks are lacking in the proposed controls.

As per the assessments, the addition of VPN and DMZ to the HGA network architecture is seen as a proactive step by the HGA executive board. However, the installation of VPN introduces new vulnerabilities and threats, increasing the risk. Controls linked to VPN were not handled in HGA's new and old controls. Because VPN poses a significant risk because employees can connect to the company's internal network from anywhere, extra traffic monitoring and firewall implementation must be considered. Meanwhile, the DMZ is used to minimize risks from outside the internal network, and every DMZ hit must be examined for any potentially suspicious activity and IOC's blocked.

To make the environment safer, the DMZ zone might be used more effectively to reduce external threats, and regular scanning of the DMZ zone is required. Many of the MOT controls that were installed failed to address important security issues like email security, antivirus, and endpoint firewalls. MOT controls are primarily focused on payroll operations and risks, but a broader view of network topology is also required. Because it has a WAN link in addition to the internet, an attacker might use lateral movement to obtain access to HGA if other agencies were hacked. As a result, IAM, Emergency Lockdown, and the isolation of affected machines must all be implemented. The firewall is also important for preventing lateral movement. Policies in the network such as local perimeter and edge perimeter, as well as DMZ, are regarded as a good solution since they improve the overall security posture, and new or old MOT controls have failed to meet the dangers posed by the above.

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

I would strongly advise using a mixed strategy approach, as evidenced by the above-mentioned document, which states that the mixed strategy is the most effective method for reducing risk to a medium level.

The outcomes are more gratifying when both risk prevention and risk response strategies are combined and handled, as the residual risk connected with the view of assets and vulnerabilities is considered.

A blended strategy, on the other hand, could not be directly approached. It is necessary to execute a risk prevention plan first, followed by a risk response strategy. As a result, work on the two types of strategies must be addressed separately in the context of real-time risk assessment execution. Because risks must be handled on a regular basis, a mixed strategy cannot be applied directly.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Controls mitigating** | **Risk Prevention Budget** | **Risk Response Budget** | **Mixed Strategy Budget** |
| Payroll Frauds | $60,000 | $40,000 | $90,000 |
| Unauthorized Access | $70,000 | $110,000 | $170,000 |
| Network Threats | $45,000 | $55,000 | $90,000 |
| Email Threats | $80,000 | $40,000 | $110,000 |
| Data Loss Prevention techniques | $90,000 | $60,000 | $140,000 |
| Data Classification and Backups | $60,000 | $80,000 | $130,000 |
| Dedicated Incident Response Team | $130,000 | $90,000 | $210,000 |
| Security Trainings for Employees | $60,000 | $70,000 | $120,000 |
| DMZ | $30,000 | $40,000 | $60,000 |
| VPN | $20,000 | $30,000 | $40,000 |
| Physical Security of Assets | $60,000 | $120,000 | $170,000 |
| **Total** | **$705,000** | **$735,000** | **$1,330,000** |

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

**$2,705,000 - $411,592 = $2,293,408**

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

**Proposed Security Budget cost for 3 Budgets:**

* Cost-benefit ratio analysis for Risk Prevention Budget
* Proposed Security Risk Budget Cost / Expected Security Risk-Benefit
* **705000 / 2293408 = 0.307**
* Cost-benefit ratio analysis for Risk Resilience Budget
* Proposed Security Risk Budget Cost / Expected Security Risk-Benefit
* **735000 / 2293408 = 0.320**
* Cost-benefit ratio analysis for Mixed Budget
* Proposed Security Risk Budget Cost / Expected Security Risk-Benefit
* **1330000 / 2293408 = 0.579**

**Reference:**

* **HGA Case Study**
* [**https://www.cisa.gov/uscert/bsi/articles/best-practices/architectural-risk-analysis**](https://www.cisa.gov/uscert/bsi/articles/best-practices/architectural-risk-analysis)

**Part B: Security Risk Management Implementation Plan**

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

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

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| **Asset ID** | **Asset Name** | **Asset Value in USD** |
| A1 | Servers | 1 million |
| A2 | Computers | 1.5 million |
| A3 | Storage Devices | $300,000 |
| A4 | Printers (2D & 3D) | $600,000 |
| A5 | Network peripherals | $500,000 |
| A6 | Personal Information | $700,000 |
| A7 | Sensitive Data & Documents | $500,000 |
| A8 | Company Reputation | Intangible |

**List of Missing Implementation Controls**

|  |
| --- |
| **Missing Controls** |
| **Identification Credentials** |
| Biometric Authentication |
| Smart Card |
| **Personal Authentication** |
| Biometric Authentication |
| Smart Card |
| **Logical Access Control Methods** |
| Passwords |
| Port Authentication using 802.1xx |
| The DoD Common Access Card |
| Alternate Login Token |
| **Biometric Systems** |
| Facial Recognition |
| Iris Recognition |

**List of Potential Vulnerabilities:**

1. Critical Data Theft
2. Potential sensitive information disclosure
3. Unauthorized Access to Servers/Workstations
4. Backdoor establishments
5. Social Engineering

**List of Potential Threats:**

1. Non-Compliance with Data Privacy
2. Loss of Confidentiality, Trustworthiness, good will, and Privacy
3. Disruption of Business lifecycles
4. Critical Data Theft
5. Potential sensitive information disclosure

**List of Possible Risks:**

1. Critical systems compromise.
2. Sensitive Data Breach.
3. Business continuity disruption.
4. Availability of most critical assets at Risk.
5. Legal and Regulatory Issues
6. Reputation loss.
7. **Network Risk Management Implementation Control and Policies**

* Enclave protection
* Firewalls
* Routers

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| **Asset ID** | **Asset Name** | **Asset Value in USD** |
| A1 | Servers | 1 million |
| A2 | Computers | 1.5 million |
| A3 | Storage Devices | $300,000 |
| A4 | Printers (2D & 3D) | $600,000 |
| A5 | Network peripherals | $500,000 |
| A6 | Personal Information | $700,000 |
| A7 | Sensitive Data & Documents | $500,000 |
| A8 | Company Reputation | Intangible |

**List of Missing Implementation Controls**

|  |
| --- |
| **Missing Controls** |
| **Enclave protection** |
| The wireless intrusion detection system |
| VPN tunnels |
| **Firewalls** |
| Application Proxy gateway |
| **Routers** |
| Securing router planes |

**List of Potential Vulnerabilities:**

1. Critical Data Theft
2. Potential sensitive information disclosure
3. Unauthorized Access to Servers/Workstations
4. Backdoor establishments
5. Social Engineering

**List of Potential Threats:**

1. Non-Compliance with Data Privacy
2. Loss of Confidentiality, Trustworthiness, good will, and Privacy
3. Disruption of Business lifecycles
4. Critical Data Theft
5. Potential sensitive information disclosure

**List of Possible Risks:**

1. Critical systems compromise.
2. Sensitive Data Breach.
3. Business continuity disruption.
4. Availability of most critical assets at Risk.
5. Legal and Regulatory Issues
6. Reputation loss.

**C) Network Management Risk Management Implementation** **Control and Policies**

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

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| **Asset ID** | **Asset Name** | **Asset Value in USD** |
| A1 | Servers | 1 million |
| A2 | Computers | 1.5 million |
| A3 | Storage Devices | $300,000 |
| A4 | Printers (2D & 3D) | $600,000 |
| A5 | Network peripherals | $500,000 |
| A6 | Personal Information | $700,000 |
| A7 | Sensitive Data & Documents | $500,000 |
| A8 | Company Reputation | Intangible |

**List of Missing Implementation Controls**

|  |
| --- |
| **Missing Controls** |
| **Ports, Protocols & Services** |
| Restricting ICMPv4 message |
| Unicast Reverse Path Forwarding |
| **Device Management** |
| Out-of-band device management |
| **Network Authentication, Authorization, and Accounting** |
| Accounting |
| Auditing |
| **Network Intrusion Detection System (NIDS)** |
| External NIDS |
| **Switches and VLANs** |
| VLAN Port Security |
| VLAN 802.1x and Management Policy Server |
| **Virtual Private Network** |
| Host to the gateway |

**List of Potential Vulnerabilities:**

1. Critical Data Theft
2. Potential sensitive information disclosure
3. Unauthorized Access to Servers/Workstations
4. Backdoor establishments
5. Social Engineering

**List of Potential Threats:**

1. Non-Compliance with Data Privacy
2. Loss of Confidentiality, Trustworthiness, good will, and Privacy
3. Disruption of Business lifecycles
4. Critical Data Theft
5. Potential sensitive information disclosure

**List of Possible Risks**

1. Critical systems compromise.
2. Sensitive Data Breach.
3. Business continuity disruption.
4. Availability of most critical assets at Risk.
5. Legal and Regulatory Issues
6. Reputation loss.

**D)Database Risk Management Implementation Control and Policies**

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

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| **Asset ID** | **Asset Name** | **Asset Value in USD** |
| A1 | Servers | 1 million |
| A2 | Computers | 1.5 million |
| A3 | Storage Devices | $300,000 |
| A4 | Printers (2D & 3D) | $600,000 |
| A5 | Network peripherals | $500,000 |
| A6 | Personal Information | $700,000 |
| A7 | Sensitive Data & Documents | $500,000 |
| A8 | Company Reputation | Intangible |

**List of Missing Implementation Controls**

|  |
| --- |
| **Missing Controls** |
| **Authentication** |
| Application User Manager |
| Database Operator |
| **Security Design and Configuration** |
| Configuration Management Process |
| **Enclave and Computing Environment** |
| Logon |
| Marking and Labeling |
| Software Development Change Controls |
| Warning Message |

**List of Potential Vulnerabilities:**

1. Critical Data Theft
2. Potential sensitive information disclosure
3. Unauthorized Access to Servers/Workstations
4. Backdoor establishments
5. Social Engineering

**List of Potential Threats:**

1. Non-Compliance with Data Privacy
2. Loss of Confidentiality, Trustworthiness, good will, and Privacy
3. Disruption of Business lifecycles
4. Critical Data Theft
5. Potential sensitive information disclosure

**List of Possible Risks**

1. Critical systems compromise.
2. Sensitive Data Breach.
3. Business continuity disruption.
4. Availability of most critical assets at Risk.
5. Legal and Regulatory Issues
6. Reputation loss.

**E) Application Risk Management Implementation Control and Policies**

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

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| **Asset ID** | **Asset Name** | **Asset Value in USD** |
| A1 | Servers | 1 million |
| A2 | Computers | 1.5 million |
| A3 | Storage Devices | $300,000 |
| A4 | Printers (2D & 3D) | $600,000 |
| A5 | Network peripherals | $500,000 |
| A6 | Personal Information | $700,000 |
| A7 | Sensitive Data & Documents | $500,000 |
| A8 | Company Reputation | Intangible |

**List of Missing Implementation Controls**

|  |
| --- |
| **Missing Controls** |
| **Application Data Handling** |
| Data Marking |
| **Authentication** |
| Authentication Credentials Protection |
| **Cryptography** |
| Use of Message Authentication Codes |
| **Input Validation** |
| Unintended Disclosure of Sensitive Information |
| **Testing** |
| Automated Tools |

**List of Potential Vulnerabilities:**

1. Critical Data Theft
2. Potential sensitive information disclosure
3. Unauthorized Access to Servers/Workstations
4. Backdoor establishments
5. Social Engineering

**List of Potential Threats:**

1. Non-Compliance with Data Privacy
2. Loss of Confidentiality, Trustworthiness, good will, and Privacy
3. Disruption of Business lifecycles
4. Critical Data Theft
5. Potential sensitive information disclosure

**List of Possible Risks**

1. Critical systems compromise.
2. Sensitive Data Breach.
3. Business continuity disruption.
4. Availability of most critical assets at Risk.
5. Legal and Regulatory Issues
6. Reputation loss.

**F) Wireless Risk Management Implementation Control and Policies**

* Wireless WAN Risk Management
* Wireless PAN Risk Management
* Wireless WAN Security
* Wireless RFID Risk Management
* Wireless PED Risk Management

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| **Asset ID** | **Asset Name** | **Asset Value in USD** |
| A1 | Servers | 1 million |
| A2 | Computers | 1.5 million |
| A3 | Storage Devices | $300,000 |
| A4 | Printers (2D & 3D) | $600,000 |
| A5 | Network peripherals | $500,000 |
| A6 | Personal Information | $700,000 |
| A7 | Sensitive Data & Documents | $500,000 |
| A8 | Company Reputation | Intangible |

**List of Missing Implementation Controls**

|  |
| --- |
| **Missing Controls** |
| **Wireless WAN Risk Management** |
| Protected Extensible Authentication Protocol (PEAP) |
| Wi-Fi Protected Access (WPA) |
| **Wireless PAN Risk Management** |
| Security models and levels |
| **Wireless RFID Risk Management** |
| Radio frequency identifier tag encryption |
| **Wireless PED Risk Management** |
| SIM cards (Subscriber Identity Module) |

**List of Potential Vulnerabilities:**

1. Critical Data Theft
2. Potential sensitive information disclosure
3. Unauthorized Access to Servers/Workstations
4. Backdoor establishments
5. Social Engineering

**List of Potential Threats:**

1. Non-Compliance with Data Privacy
2. Loss of Confidentiality, Trustworthiness, good will, and Privacy
3. Disruption of Business lifecycles
4. Critical Data Theft
5. Potential sensitive information disclosure

**List of Possible Risks**

1. Critical systems compromise.
2. Sensitive Data Breach.
3. Business continuity disruption.
4. Availability of most critical assets at Risk.
5. Legal and Regulatory Issues
6. Reputation loss.

**List of Cybersecurity Implementation controls at Boston Orthopedics**

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

|  |
| --- |
| **Identification Credentials** |
| ID card |
| Username & Password |
| Wallet ID |
| Digital Certificates |
| Biometric Authentication |
| Social Security Number |
| Photograph |
| Smart Card |
| MFA |
| **Personal Authentication** |
| ID card |
| Username & Password |
| Wallet ID |
| Biometric Authentication |
| Social Security Number |
| Photograph |
| Smart Card |
| MFA |
| **Authorization** |
| Privileged user access |
| Access Control Lists (ACL) |
| Active Directory (AD) |
| Access Control Policies |
| **Logical Access Control Methods** |
| Network Architecture Controls |
| Logical Network Port Security |
| PKI |
| Digital Certificates |
| Passwords |
| Port Authentication using 802.1xx |
| MFA |
| The DoD Common Access Card |
| Alternate Login Token |
| **Physical Access Control Methods** |
| Entry points |
| Cameras |
| Work Bay access and Floor access |
| Critical Asset physical access |
| Special Badges & Tangible Tokens |
| Physical Intrusion Detection Systems |
| **Biometric Systems** |
| Fingerprint Scanning |
| Facial Recognition |
| Iris Recognition |

1. **Network Risk Management Implementation Control and Policies**

|  |
| --- |
| **Implementation Controls** |
| **Enclave protection** |
| Firewalls |
| Routers |
| Intrusion Detection System |
| Intrusion Prevention systems |
| Demilitarized Zone |
| Test Access Points |
| Load balancers |
| The wireless intrusion detection system |
| VPN tunnels |
| **Firewalls** |
| Packet filtering firewall |
| DNS Security |
| Deep packet inspection firewall |
| Application Proxy gateway |
| Hybrid technology firewall |
| Proxy servers |
| URL Filtering |
| **Routers** |
| Route table integrity |
| Securing router planes |

**C) Network Management Risk Management Implementation Control and Policies**

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

**D) Database Risk Management Implementation Control and Policies**

|  |
| --- |
| **Cybersecurity Implementation Controls** |
| **Authentication** |
| User Accounts |
| Database Administrator (DBA) |
| Application Owner |
| Application User Manager |
| Application Account |
| Database Auditor |
| Database Operator |
| Access Control Lists |
| Passwords |
| Certificates |
| External Authentication |
| Credential Storage |
| **Authorization** |
| Role Based Access Control |
| Renaming Default Accounts |
| **Confidentiality** |
| Data Encryption |
| Encryption of Application Codes |
| Data File Encryption |
| **Data Integrity** |
| Transaction Log |
| Data Integrity |
| **Auditing** |
| Audit Log Protection |
| Audit Log Retention |
| Audit Reporting |
| **Replication and Federation** |
| Database Replication |
| Database Links |
| **Clustering** |
| Database Clustering |
| Principle of Least Privilege |
| Trail of Accountability |
| Protected Communication Path |
| **Backup and Recovery** |
| DBMS Backup |
| Testing and Maintenance |
| Authentication and Authorization |
| **Operating System Authorization** |
| Dedicated directories and files |
| Dedicated operating systems accounts |
| Updated Database Software |
| **Application Protections** |
| Audit of Elevated Privileges |
| Input Validation |
| Authentication Method |
| Least Privilege Mechanism |
| **Network Protection** |
| Network Access |
| Time and Count Time Limits |
| Encrypted and Protected Data Across Network |
| **Security Design and Configuration** |
| Procedural Review |
| Configuration Specifications |
| Compliance Testing |
| Functional Architecture for IS Applications |
| Non-Repudiation |
| Partitioning the Application |
| Ports, Protocols, and Services |
| Configuration Management Process |
| IA Documentation |
| System Library Management Controls |
| Security Structure Support Partitioning |
| System State Changes |
| Software Baseline |
| Group Identification and Authentication |
| Individual Identification and Authentication |
| Key Management |
| Token and Certificate Standards |
| **Enclave and Computing Environment** |
| Access for Need to Know |
| Audit Record Content |
| Audit Trail, Monitoring, Analysis, and Reporting |
| Changes to Data |
| Encryption for Confidentiality |
| Data Change Controls |
| Interconnections among systems and enclaves |
| Audit of Security Label Changes |
| Logon |
| Privileged Account Control |
| Marking and Labeling |
| Production code change controls |
| Resource Control |
| Security Configuration Compliance |
| Audit Reduction and Report Generation |
| Software Development Change Controls |
| Warning Message |
| Boundary Defense |
| Remote Access for Privileged Functions |
| **Business Continuity** |
| Protection of Backup and Restoration Assets |
| Data Backup Procedures |
| Disaster Recovery and Planning |
| Backup copies of Critical Software |
| Trusted Recovery |
| **Vulnerability and Incident Management** |
| Vulnerability Management |

**E) Application Risk Management Implementation Control and Policies**

|  |
| --- |
| **Cybersecurity Implementation Controls** |
| **Application Data Handling** |
| Database Management Systems |
| Data Storage |
| In-Memory Data Handling |
| Data Transmission |
| Data Integrity |
| Data Marking |
| **Authentication** |
| Server Authentication |
| User Authentication |
| Signed Code Identification |
| Standalone Application Authentication |
| Server Application Authentication |
| Client Application Authentication |
| Client-Server Application Authentication |
| Application Component Authentication |
| PKI Certificate Validation |
| Password Complexity and Maintenance |
| Authentication Credentials Protection |
| **Cryptography** |
| Symmetric Cryptography |
| Use of Message Authentication Codes |
| Use of Digital Signatures |
| **User Accounts** |
| Account Rules |
| Account Lockout Policy |
| When revoking access |
| Avoiding Duplicate Accounts |
| Application Sessions |
| Access Control |
| **Input Validation** |
| User Input Validation |
| Web Encoding |
| Race Condition |
| Static Analysis |
| Unintended Disclosure of Sensitive Information |
| **Auditing** |
| Notification and Auditing Content |
| Protecting Audit Trails |
| **Configuration Management** |
| Configuration Management |
| Limit Unauthorized Individuals |
| **Testing** |
| Test Plans and Procedures |
| Automated Tools |
| **Deployment** |
| Documentation |
| Auditing |

**F) Wireless Risk Management Implementation Control and Policies**

|  |
| --- |
| **Cybersecurity Implementation Controls** |
| **Wireless WAN Risk Management** |
| IEEE 802 11x Extensible Authentication Protocol |
| EAP-Transport Layer Security |
| EAP-Tunneling Transport Layer Security |
| Protected Extensible Authentication Protocol (PEAP) |
| Network Separation |
| Virtual private network (VPN) |
| User Authentication and Data Encryption Services |
| Wi-Fi Protected Access (WPA) |
| Service Set Identifier (SSID) |
| Access point and client identification |
| RSN, WRAP and CCMP protocol |
| **Wireless PAN Risk Management** |
| Bluetooth specification |
| Device level authentication |
| Data encryption |
| Pairing |
| CIA and authorization |
| Security models and levels |
| Secure simple pairing |
| Key Management |
| **Wireless WAN Security** |
| Use of cellular digital packet data (CDPD) |
| **Wireless RFID Risk Management** |
| Radio frequency identifier tag encryption |
| **Wireless PED Risk Management** |
| SIM cards (Subscriber Identity Module) |
| Wireless Email |
| PDA Security |

**Comparison of the Implementation Controls discussed in the class with your company’s existing Cybersecurity Implementation Controls**

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

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Status** |
| **Identification Credentials** | |
| ID card | Present |
| Username & Password | Present |
| Wallet ID | Present |
| Digital Certificates | Present |
| Biometric Authentication | Absent |
| Social Security Number | Present |
| Photograph | Present |
| Smart Card | Absent |
| MFA | Present |
| **Personal Authentication** | |
| ID card | Present |
| Username & Password | Present |
| Wallet ID | Present |
| Biometric Authentication | Absent |
| Social Security Number | Present |
| Photograph | Present |
| Smart Card | Absent |
| MFA | Present |
| **Authorization** | |
| Privileged user access | Present |
| Access Control Lists (ACL) | Present |
| Active Directory (AD) | Present |
| Access Control Policies | Present |
| **Logical Access Control Methods** | |
| Network Architecture Controls | Present |
| Logical Network Port Security | Present |
| PKI | Present |
| Digital Certificates | Present |
| Passwords | Absent |
| Port Authentication using 802.1xx | Absent |
| MFA | Present |
| The DoD Common Access Card | Absent |
| Alternate Login Token | Absent |
| **Physical Access Control Methods** | |
| Entry points | Present |
| Cameras | Present |
| Work Bay access and Floor access | Present |
| Critical Asset physical access | Present |
| Special Badges & Tangible Tokens | Present |
| Physical Intrusion Detection Systems | Present |
| **Biometric Systems** | |
| Fingerprint Scanning | Present |
| Facial Recognition | Absent |
| Iris Recognition | Absent |

1. **Network Risk Management Implementation Control and Policies**

|  |  |
| --- | --- |
| **Implementation Controls** | **Implementation Status** |
| **Enclave protection** | |
| Firewalls | Present |
| Routers | Present |
| Intrusion Detection System | Present |
| Intrusion Prevention systems | Present |
| Demilitarized Zone | Present |
| Test Access Points | Present |
| Load balancers | Present |
| The wireless intrusion detection system | Absent |
| VPN tunnels | Absent |
|  |  |
| **Firewalls** | |
| Packet filtering firewall | Present |
| DNS Security | Present |
| Deep packet inspection firewall | Present |
| Application Proxy gateway | Absent |
| Hybrid technology firewall | Present |
| Proxy servers | Present |
| URL Filtering | Present |
|  |  |
| **Routers** | |
| Route table integrity | Present |
| Securing router planes | Absent |

1. **Network Management Risk Management Implementation Control and Policies**

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

1. **Database Risk Management Implementation Control and Policies**

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Status** |
| **Authentication** |  |
| User Accounts | Present |
| Database Administrator(DBA) | Present |
| Application Owner | Present |
| Application User Manager | Absent |
| Application Account | Present |
| Database Auditor | Present |
| Database Operator | Absent |
| Access Control Lists | Present |
| Passwords | Present |
| Certificates | Present |
| External Authentication | Present |
| Credential Storage | Present |
| **Authorization** |  |
| Role Based Access Control | Present |
| Renaming Default Accounts | Present |
| **Confidentiality** |  |
| Data Encryption | Present |
| Encryption of Application Codes | Present |
| Data File Encryption | Present |
| **Data Integrity** |  |
| Transaction Log | Present |
| Data Integrity | Present |
| **Auditing** |  |
| Audit Log Protection | Present |
| Audit Log Retention | Present |
| Audit Reporting | Present |
| **Replication and Federation** |  |
| Database Replication | Present |
| Database Links | Present |
| **Clustering** |  |
| Database Clustering | Present |
| Principle of Least Privilege | Present |
| Trail of Accountability | Present |
| Protected Communication Path | Present |
| **Backup and Recovery** |  |
| DBMS Backup | Present |
| Testing and Maintenance | Present |
| Authentication and Authorization | Present |
| **Operating System Authorization** |  |
| Dedicated directories and files | Present |
| Dedicated operating systems accounts | Present |
| Updated Database Software | Present |
| **Application Protections** |  |
| Audit of Elevated Privileges | Present |
| Input Validation | Present |
| Authentication Method | Present |
| Least Privilege Mechanism | Present |
| **Network Protection** |  |
| Network Access | Present |
| Time and Count Time Limits | Present |
| Encrypted and Protected Data Across Network | Present |
| **Security Design and Configuration** |  |
| Procedural Review | Present |
| Configuration Specifications | Present |
| Compliance Testing | Present |
| Functional Architecture for IS Applications | Present |
| Non-Repudiation | Present |
| Partitioning the Application | Present |
| Ports, Protocols, and Services | Present |
| Configuration Management Process | Absent |
| IA Documentation | Present |
| System Library Management Controls | Present |
| Security Structure Support Partitioning | Present |
| System State Changes | Present |
| Software Baseline | Present |
| Group Identification and Authentication | Present |
| Individual Identification and Authentication | Present |
| Key Management | Present |
| Token and Certificate Standards | Present |
| **Enclave and Computing Environment** |  |
| Access for Need to Know | Present |
| Audit Record Content | Present |
| Audit Trail, Monitoring, Analysis, and Reporting | Present |
| Changes to Data | Present |
| Encryption for Confidentiality | Present |
| Data Change Controls | Present |
| Interconnections among systems and enclaves | Present |
| Audit of Security Label Changes | Present |
| Logon | Absent |
| Privileged Account Control | Present |
| Marking and Labeling | Absent |
| Production code change controls | Present |
| Resource Control | Present |
| Security Configuration Compliance | Present |
| Audit Reduction and Report Generation | Present |
| Software Development Change Controls | Absent |
| Warning Message | Absent |
| Boundary Defense | Present |
| Remote Access for Privileged Functions | Present |
| **Business Continuity** |  |
| Protection of Backup and Restoration Assets | Present |
| Data Backup Procedures | Present |
| Disaster Recovery and Planning | Present |
| Backup copies of Critical Software | Present |
| Trusted Recovery | Present |
| **Vulnerability and Incident Management** |  |
| Vulnerability Management | Present |

1. **Application Risk Management Implementation Control and Policies**

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Status** |
| **Application Data Handling** |  |
| Database Management Systems | Present |
| Data Storage | Present |
| In-Memory Data Handling | Present |
| Data Transmission | Present |
| Data Integrity | Present |
| Data Marking | Absent |
| **Authentication** |  |
| Server Authentication | Present |
| User Authentication | Present |
| Signed Code Identification | Present |
| Standalone Application Authentication | Present |
| Server Application Authentication | Present |
| Client Application Authentication | Present |
| Client-Server Application Authentication | Present |
| Application Component Authentication | Present |
| PKI Certificate Validation | Present |
| Password Complexity and Maintenance | Present |
| Authentication Credentials Protection | Absent |
| **Cryptography** |  |
| Symmetric Cryptography | Present |
| Use of Message Authentication Codes | Absent |
| Use of Digital Signatures | Present |
| **User Accounts** |  |
| Account Rules | Present |
| Account Lockout Policy | Present |
| When revoking access | Present |
| Avoiding Duplicate Accounts | Present |
| Application Sessions | Present |
| Access Control | Present |
| **Input Validation** |  |
| User Input Validation | Present |
| Web Encoding | Present |
| Race Condition | Present |
| Static Analysis | Present |
| Unintended Disclosure of Sensitive Information | Absent |
| **Auditing** |  |
| Notification and Auditing Content | Present |
| Protecting Audit Trails | Present |
| **Configuration Management** |  |
| Configuration Management | Present |
| Limit Unauthorized Individuals | Present |
| **Testing** |  |
| Test Plans and Procedures | Present |
| Automated Tools | Absent |
| **Deployment** |  |
| Documentation | Present |
| Auditing | Present |

1. **Wireless Risk Management Implementation Control and Policies**

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Status** |
| **Wireless WAN Risk Management** |  |
| IEEE 802 11x Extensible Authentication Protocol | Present |
| EAP-Transport Layer Security | Present |
| EAP-Tunneling Transport Layer Security | Present |
| Protected Extensible Authentication Protocol (PEAP) | Absent |
| Network Separation | Present |
| Virtual private network (VPN) | Present |
| User Authentication and Data Encryption Services | Present |
| Wi-Fi Protected Access (WPA) | Absent |
| Service Set Identifier (SSID) | Present |
| Access point and client identification | Present |
| RSN, WRAP and CCMP protocol | Present |
| **Wireless PAN Risk Management** |  |
| Bluetooth specification | Present |
| Device level authentication | Present |
| Data encryption | Present |
| Pairing | Present |
| CIA and authorization | Present |
| Security models and levels | Absent |
| Secure simple pairing | Present |
| Key Management | Present |
| **Wireless WAN Security** |  |
| Use of cellular digital packet data (CDPD) | Present |
| **Wireless RFID Risk Management** |  |
| Radio frequency identifier tag encryption | Absent |
| **Wireless PED Risk Management** |  |
| SIM cards (Subscriber Identity Module) | Absent |
| Wireless Email | Present |
| PDA Security | Present |

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| **Asset ID** | **Asset Name** | **Asset Value in USD** |
| A1 | Servers | 1 million |
| A2 | Computers | 1.5 million |
| A3 | Storage Devices | $300,000 |
| A4 | Printers (2D & 3D) | $600,000 |
| A5 | Network peripherals | $500,000 |
| A6 | Personal Information | $700,000 |
| A7 | Sensitive Data & Documents | $500,000 |
| A8 | Company Reputation | Intangible |

**List of Potential Vulnerabilities for critical assets where cybersecurity Implementation Controls are missing**

* Sensitive data exposure
* Information Theft
* Unauthorized access
* Weak access
* Network compromise and weak network configurations
* Critical Data Theft
* Potential sensitive information disclosure
* Unauthorized Access to Servers/Workstations
* Backdoor establishments
* Social Engineering

**List of Potential threats due to Vulnerabilities of Critical Assets**

* Loss of Confidentiality, Privacy, Credibility and Nonrepudiation.
* Data Privacy and Availability
* Disruption of Business lifecycles
* Legal and regulatory issues
* Information theft
* Integrity & Data Privacy Loss
* Non-Compliance with Data Privacy
* Loss of Confidentiality, Trustworthiness, good will, and Privacy
* Disruption of Business lifecycles
* Critical Data Theft
* Potential sensitive information disclosure

**List of Potential Risks for critical assets where cybersecurity Implementation Controls are missing**

* Critical systems compromise.
* Sensitive Data Breach.
* Business continuity disruption.
* Availability of most critical assets at Risk.
* Legal and Regulatory Issues
* Reputation loss.
* Provide access to critically sensitive data to Bad vectors
* The smart card acts as a physical access token and is unique.
* Provide access to critically sensitive data to Bad vectors.
* Can make systems/servers compromise easily if ports were not blocked and monitored.
* Information theft is made easy if the DoD common access card is not present.

**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 necessary to identify and categorize information assets according to their level of criticality. Audits of information security and compliance should be undertaken on a regular basis.

• To secure the organization's total information security infrastructure, it should consider adopting the ISO 27001 — Information Security Management Systems standard, which will assist in the implementation of all information security rules.

• Data confidentiality and integrity can be preserved by encrypting data in storage and transmission. Individual PCs and entire networks can be protected by firewalls from security threats. Setting up rules can be beneficial.

• It is critical to reinforce the system's authentication infrastructure to prevent illegal access. To restrict any allowed access, multifactor authentication with time-based one-time passwords and biometric elements should be introduced.

• Using a zero-trust access control strategy will reduce the number of data leaks and prevent employees from gaining access to critical information.

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

• Check that the antivirus and intrusion prevention systems are set up to respond quickly in the event of an occurrence. Validate and test the systems and networks to ensure that they are all operational.

• Create a Business Continuity Plan that outlines the measures to be followed before, during, and after a disruptive event that results in the loss of Information System availability.

• Plan for the incident's isolation and containment. Ascertain that the incident response team is working on the event's root cause analysis.

• To identify any application faults, check logs created by multiple systems and applications. Examine the error logs of the operators to see if there are any resource or operational issues. To avoid the loss of mission-critical services, applications, and data, daily backups of mission-critical services, applications, and data should be performed.

• Have a Disaster Recovery Plan and Contingency Plan in place that has been recorded and approved.

**Applicable Government Regulations and Industry Standards**

**HIPAA**

As my organization is a medical devices manufacturing company, it must follow the HIPAA guidelines and all the employees have to take the HIPAA related trainings. Usually HIPAA Privacy Regulations, HIPAA Security Regulations, and HIPAA Breach Notification Regulations are all governed by HIPAA.

In the event of a cyber-related security incident, a HIPAA covered firm or its business associate must take a few actions. All of the below check marks must be met in the event of a cyber-attack or other comparable situation.

• All mitigation and response processes, as well as a contingency plan, should be in place. To put an end to the situation, any technical or other issues must be resolved. Must take precautions to prevent any unauthorized disclosure of protected health information.

• You should notify other law enforcement agencies about the crime. Law enforcement, the Federal Bureau of Investigation (FBI), and/or the Secret Service are all possible candidates. Unless the HIPAA Privacy Rule allows otherwise, such reports should not include protected health information.

• All cyber danger indicators should be reported to federal and information-sharing and analysis organizations (ISAOS), such as the Department of Homeland Security and the Department of Health and Human Services.

• Must notify impacted individuals and the media as soon as feasible, but no later than 60 days after discovering a breach impacting 500 or more people, and disclose the breach to the Office of Civil Rights, OCR, unless a law enforcement official has sought a delay in reporting. Unless the information was encrypted by the entity at the time of the incident or the entity determines, through a written risk assessment, that there was a low probability that the information was compromised during the breach, OCR presumes all cyber-related security incidents where protected health information was accessed, acquired, used, or disclosed are reportable breaches.

• Protected health information (PHI) should not be disclosed unless it is specifically requested.

**ISO/IEC 27001**

**Structure of the standard**

SO/IEC 27001 formally specifies an Information Security Management System, a governance arrangement comprising a structured suite of activities with which to manage information risks (called ‘information security risks’ in the standard).

The ISMS is an overarching framework through which management identifies, evaluates and treats (addresses) the organization’s information risks. The ISMS ensures that the security arrangements are fine-tuned to keep pace with changes to the security threats, vulnerabilities and business impacts - an important aspect in such a dynamic field, and a key advantage of ISO27k’s flexible risk-driven approach as compared to, say, PCI-DSS.

The standard covers all types of organizations (e.g. commercial enterprises, government agencies, non-profits) of all sizes (from micro-businesses to huge multinationals) in all industries (e.g. retail, banking, defense, healthcare, education and government). This is clearly a very wide brief.

ISO/IEC 27001:2013 has the following sections:

1. Introduction - the standard describes a process for systematically managing information risks.
2. Scope - it specifies generic ISMS requirements suitable for organizations of any type, size or nature.
3. Normative references - only ISO/IEC 27000 is considered absolutely essential to users of ’27001: the remaining ISO27k standards are optional.
4. Terms and definitions - see ISO/IEC 27000.
5. Context of the organization - understanding the organizational context, the needs and expectations of ‘interested parties’ and defining the scope of the ISMS. Section 4.4 states very plainly that “The organization shall establish, implement, maintain and continually improve” the ISMS.
6. Leadership - top management must demonstrate leadership and commitment to the ISMS, mandate policy, and assign information security roles, responsibilities and authorities.
7. Planning - outlines the process to identify, analyze and plan to treat information risks, and clarify the objectives of information security.
8. Support - adequate, competent resources must be assigned, awareness raised, documentation prepared and controlled.
9. Operation - a bit more detail about assessing and treating information risks, managing changes, and documenting things (partly so that they can be audited by the certification auditors).
10. Performance evaluation - monitor, measure, analyze and evaluate/audit/review the information security controls, processes and management system, systematically improving things where necessary.
11. Improvement - address the findings of audits and reviews (e.g. nonconformities and corrective actions), make continual refinements to the ISMS.

**Sarbanes-Oxley Act**

The Sarbanes-Oxley Act of 2002, often simply called SOX or Sarbox, is U.S. law meant to protect investors from fraudulent accounting activities by corporations. Sarbanes-Oxley was enacted after several major accounting scandals in the early 2000’s perpetrated by companies such as Enron, Tyco, and WorldCom. So what is SOX? The law mandates strict reforms to improve financial disclosures from corporations and prevent accounting fraud. It also covers issues such as auditor independence, corporate governance, internal control assessment, and enhanced financial disclosure.

The law is named for the two congressmen who drafted it, Paul Sarbanes and Michael Oxley. The U.S. Securities and Exchange Commission (SEC) administers the act.

Though Sarbanes-Oxley does not call out any specific IT requirements, the law does have a great impact on information systems – and in particular the security of those systems – owed to the fact that the financial information covered under the law is processed and stored by IT systems. Section 404 in particular has had very costly implications for publicly-traded companies as it is expensive to establish, maintain, and validate the required internal controls.

Sarbanes-Oxley is arranged into 11 titles. As far as SOX compliance is concerned, the most important sections within these are often considered to be 302, 404, 409, 802 and 906.

* Section 302 – Corporate Responsibility for Financial Reports – Every public company is required to file periodic financial reports with the SEC, and the principal executive officer and the principal financial officer must sign each report to indicate they have reviewed it and they certify that the report does not contain any untrue statements and does not omit any material information. In addition, the signers of the report are responsible for establishing and maintaining internal sox controls and must have validated those controls within 90 days prior to issuing the report.
* Section 404 – Management Assessment of Internal Controls – All annual financial reports must include an Internal Control Report stating that management is responsible for an “adequate” internal control structure, and an assessment by management of the effectiveness of the control structure. Any shortcomings in these SOX controls also must be reported. In addition, registered external auditors must attest to the accuracy of the company management’s assertion that internal accounting controls are in place, operational and effective.
* Section 409 – Real Time Issuer Disclosures – Companies are required to disclose to the public in a timely manner any material changes in the financial condition or operations of the company in the interest of protecting investors and the public.
* Section 802 – Criminal Penalties for Altering Documents – Anyone who knowingly alters, destroys, mutilates, conceals, covers up, falsifies, or makes a false entry in any record, document, or tangible object with the intent to impede, obstruct, or influence the investigation or proper administration of matters before the SEC can be fined, imprisoned for no more than 20 years, or both.
* Section 906 – Corporate Responsibility for Financial Reports – The criminal penalty for certifying a misleading or fraudulent financial report can be upwards of $5 million in fines and 20 years in prison.

**Gramm-Leach-Bliley Act**

The Gramm-Leach-Bliley Act requires financial institutions—which includes colleges and universities—to protect the privacy of their customers, including customers' nonpublic, personal information. Because universities are governed by the GLBA, Western Michigan University has a responsibility to secure the personal records of its students and employees. To ensure this protection, the GLBA mandates all institutions establish appropriate administrative, technical and physical safeguards.

By customer information, the Gramm-Leach-Bliley Act means information typically gathered in connection with obtaining a financial product or service; this includes but is not limited to include names, addresses, phone numbers, bank and credit card account numbers, income and credit histories and Social Security numbers.

In an effort to set safeguarding standards the GLBA directs that all financial institutions implement an Information Security Program and designate a program coordinator.

The Information Security Program must include five main elements:

1. Designation of an employee or employees as coordinator of the information security program.
2. Identification of internal and external risks to the security and confidentiality of customer information and evaluation of current safeguards.
3. Employee training.
4. Oversight of service providers.
5. Evaluation of the information security program.
6. The following are the objectives of the Information Security Program for the Gramm-Leach-Bliley Act; Health Insurance Portability and Accountability Act of 1996; Family Education and Privacy Act of 1974; and Identity Theft Red Flags Act of 2003:
7. Ensure the security and confidentiality of customer information in compliance with applicable GLBA rules as published by the Federal Trade Commission.
8. Provide administrative, physical and technical safeguards to ensure compliance with the HIPAA Security Rule.
9. Implement a Red Flag program that is designed to detect identity theft in day-to-day university operations.
10. Ensure the privacy and confidentiality of student information in compliance with Federal law, including both technical and administrative safeguards.
11. Safeguard against anticipated threats to the security or integrity of protected electronic data.
12. Guard against unauthorized access to or use of protected data that could result in harm or inconvenience to any customer.

**Federal Information Security Management Act (FISMA)**

The Federal Information Security Management Act (FISMA) [FISMA 2002], part of the E-Government Act (Public Law 107-347) was passed in December 2002. FISMA 2002 requires each federal agency to develop, document, and implement an agency-wide program to provide information security for the information and systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other sources.

The Federal Information Security Modernization Act of 2014 amends FISMA 2002, by providing several modifications that modernize federal security practices to address evolving security concerns. These changes result in less overall reporting, strengthens the use of continuous monitoring in systems, increases focus on the agencies for compliance and reporting that is more focused on the issues caused by security incidents. FISMA 2014 also required the Office of Management and Budget (OMB) to amend/revise OMB Circular A-130 to eliminate inefficient and wasteful reporting and reflect changes in law and advances in technology.

The NIST Risk Management Framework (RMF) provides a flexible, holistic, and repeatable 7-step process to manage security and privacy risk and links to a suite of NIST standards and guidelines to support implementation of risk management programs to meet the requirements of the Federal Information Security Modernization Act (FISMA).

The risk-based approach of the NIST RMF helps an organization:

Prepare for risk management through essential activities critical to design and implementation of a risk management program.

Categorize systems and information based on an impact analysis.

Select a set of the NIST SP 800-53 controls to protect the system based on risk assessments.

Implement the controls, and documents how the controls are deployed.

Assess the control implementation to determine if the controls are in place, operating as intended, and producing the desired results to manage risk.

Authorize the system to operate by a senior-level official that understanding the controls in place to manage risk and any residual risk.

Continuously monitor control implementation and changes to the risks to the system.

**General Data Protection Regulation (GDPR)**

The purpose of the GDPR is to impose a uniform data security law on all EU members, so that each member state no longer needs to write its own data protection laws and laws are consistent across the entire EU. In addition to EU members, it is important to note that any company that markets goods or services to EU residents, regardless of its location, is subject to the regulation. As a result, GDPR will have an impact on data protection requirements globally.

The General Data Protection Regulation (GDPR), agreed upon by the European Parliament and Council in April 2016, will replace the Data Protection Directive 95/46/ec in Spring 2018 as the primary law regulating how companies protect EU citizens' personal data. Companies that are already in compliance with the Directive must ensure that they are also compliant with the new requirements of the GDPR before it becomes effective on May 25, 2018. Companies that fail to achieve GDPR compliance before the deadline will be subject to stiff penalties and fines.

GDPR requirements apply to each member state of the European Union, aiming to create more consistent protection of consumer and personal data across EU nations. Some of the key privacy and data protection requirements of the GDPR include:

* Requiring the consent of subjects for data processing
* Anonymizing collected data to protect privacy
* Providing data breach notifications
* Safely handling the transfer of data across borders
* Requiring certain companies to appoint a data protection officer to oversee GDPR compliance

The GDPR itself contains 11 chapters and 91 articles. The following are some of the chapters and articles that have the greatest potential impact on security operations:

* Articles 17 & 18 – Articles 17 and 18 of the GDPR give data subjects more control over personal data that is processed automatically. The result is that data subjects may transfer their personal data between service providers more easily (also called the “right to portability”), and they may direct a controller to erase their personal data under certain circumstances (also called the “right to erasure”).
* Articles 23 & 30 – Articles 23 and 30 require companies to implement reasonable data protection measures to protect consumers’ personal data and privacy against loss or exposure.
* Articles 31 & 32 – Data breach notifications play a large role in the GDPR text. Article 31 specifies requirements for single data breaches: controllers must notify Supervising Authorities (SA)s of a personal data breach within 72 hours of learning of the breach and must provide specific details of the breach such as the nature of it and the approximate number of data subjects affected. Article 32 requires data controllers to notify data subjects as quickly as possible of breaches when the breaches place their rights and freedoms at high risk.
* Articles 33 & 33a – Articles 33 and 33a require companies to perform Data Protection Impact Assessments to identify risks to consumer data and Data Protection Compliance Reviews to ensure those risks are addressed.
* Article 35 – Article 35 requires that certain companies appoint data protection officers. Specifically, any company that processes data revealing a subject’s genetic data, health, racial or ethnic origin, religious beliefs, etc. must designate a data protection officer; these officers serve to advise companies about compliance with the regulation and act as a point of contact with SAs. Some companies may be subjected to this aspect of the GDPR simply because they collect personal information about their employees as part of human resources processes.
* Articles 36 & 37 – Articles 36 and 37 outline the data protection officer position and its responsibilities in ensuring GDPR compliance as well as reporting to Supervisory Authorities and data subjects.
* Article 45 – Article 45 extends data protection requirements to international companies that collect or process EU citizens’ personal data, subjecting them to the same requirements and penalties as EU-based companies.
* Article 79 – Article 79 outlines the penalties for GDPR non-compliance, which can be up to 4% of the violating company’s global annual revenue depending on the nature of the violation.

**Rank Asset Risks and Vulnerability Risks for your company across Access Control, Network Infrastructure, Network Infrastructure Management, Database, Applications and wireless**

|  |  |  |
| --- | --- | --- |
| **Topic** | **Top 5 Risks** | **Top 5 Vulnerabilities** |
| **Access Control** | Provide access to critically sensitive data to Bad vectors. The smart card acts as a physical access token and is unique. | Critical Data Theft |
| Can make systems/servers compromise easily if ports were not blocked and monitored. | Potential sensitive information disclosure |
| Information theft is made easy if the DoD common access card is not present. | Unauthorized Access to Servers/Workstations |
| Password controls have to be followed to not Provide access to critically sensitive data to Bad vectors | Backdoor establishments |
| The latest technologies are harder to crack, older techniques might leverage bad vectors. | Social Engineering |
| **Network Infrastructure** | Provide access to critically sensitive data to Bad vectors. Wireless sessions need to be secured against man-in-the-middle attacks. | Weak network infrastructure |
| Information Theft, Unauthorized access, Weak access, Sensitive data exposure | Potential sensitive information disclosure |
| Weak network infrastructure, Information Theft, Unauthorized access | Unauthorized Access to Servers/Workstations |
| Provide access to critically sensitive data to Bad vectors. Router planes must be secured in order to minimize attacks on routers. | Backdoor establishments |
| Information theft is made easy if the DoD controls not present. | Unprotected wireless network |
| **Network Infrastructure Management** | Provide access to critically sensitive data to Bad vectors. | Sensitive data exposure and Information Theft |
| Weak network infrastructure, Information Theft, Unauthorized access | Unprotected router planes |
| Wireless sessions need to be secured against man-in-the-middle attacks. | DDOS Attacks |
| Information Theft, Unauthorized access, Weak access, Sensitive data exposure | Unauthorized access and Weak access |
| Wireless sessions need to be secured against man-in-the-middle attacks. | Unprotected wireless network |
| **Database** | Provide access to critically sensitive data to Bad vectors. | Information Theft |
| Wireless sessions need to be secured against man-in-the-middle attacks. | Unauthorized access |
| Information Theft and Unauthorized access | Unprotected wireless network |
| Weak database infrastructure | Weak access |
| Information Theft, Unauthorized access, Weak access, Sensitive data exposure | Sensitive data exposure |
| **Application** | Provide access to critically sensitive data to Bad vectors. Wireless sessions need to be secured against man-in-the-middle attacks. | Unauthorized Access to Servers/Workstations |
| Wireless sessions need to be secured against man-in-the-middle attacks. | Backdoor establishments |
| Information Theft, Unauthorized access, Weak access, Sensitive data exposure | Social Engineering |
| Disruption of Business lifecycles | Weak network infrastructure |
| Can make systems/servers compromise easily if ports were not blocked and monitored. | Potential sensitive information disclosure |
| **Wireless** | Weak network infrastructure, Information Theft, Unauthorized access | Backdoor establishments |
| Wireless sessions need to be secured against man-in-the-middle attacks. | Unprotected wireless network |
| Password controls have to be followed to not Provide access to critically sensitive data to Bad vectors | Sensitive data exposure and Information Theft |
| Can make systems/servers compromise easily if ports were not blocked and monitored. | Unprotected router planes |
| The latest technologies are harder to crack, older techniques might leverage bad vectors. | DDOS Attacks |

**List of Top 5 Vulnerabilities:**

* Critical Data Theft
* Potential sensitive information disclosure
* Unauthorized Access to Servers/Workstations
* Backdoor establishments
* Social Engineering

**List of Top 5 Risks**

* Critical systems compromise.
* Sensitive Data Breach.
* Business continuity disruption.
* Availability of most critical assets at Risk.
* Legal and Regulatory Issues
* Reputation loss.

**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 necessary to identify and categorize information assets according to their level of criticality. Audits of information security and compliance should be undertaken on a regular basis.

• To secure the organization's total information security infrastructure, it should consider adopting the ISO 27001 — Information Security Management Systems standard, which will assist in the implementation of all information security rules.

• Data confidentiality and integrity can be preserved by encrypting data in storage and transmission. Individual PCs and entire networks can be protected by firewalls from security threats. Setting up rules can be beneficial.

• It is critical to reinforce the system's authentication infrastructure to prevent illegal access. To restrict any allowed access, multifactor authentication with time-based one-time passwords and biometric elements should be introduced.

• Using a zero-trust access control strategy will reduce the number of data leaks and prevent employees from gaining access to critical information.

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

• Check that the antivirus and intrusion prevention systems are set up to respond quickly in the event of an occurrence. Validate and test the systems and networks to ensure that they are all operational.

• Create a Business Continuity Plan that outlines the measures to be followed before, during, and after a disruptive event that results in the loss of Information System availability.

• Plan for the incident's isolation and containment. Ascertain that the incident response team is working on the event's root cause analysis.

• To identify any application faults, check logs created by multiple systems and applications. Examine the error logs of the operators to see if there are any resource or operational issues. To avoid the loss of mission-critical services, applications, and data, daily backups of mission-critical services, applications, and data should be performed.

• Have a Disaster Recovery Plan and Contingency Plan in place that has been recorded and approved.

**Cybersecurity Workspace Risk Management Implementation**

**List of Cybersecurity Specialty Areas that exist at Boston Orthopedics**

|  |
| --- |
| **NICE Specialty Area** |
| Risk Management (RSK) |
| Software Development (DEV) |
| Systems Architecture (ARC) |
| Technology R&D (TRD) |
| Systems Requirements Planning (SRP) |
| Test and Evaluation (TST) |
| Systems Development (SYS) |
| Data Administration (DTA) |
| Knowledge Management (KMG) |
| Customer Service and Technical Support (STS) |
| Network Services (NET) |
| Systems Administration (ADM) |
| Systems Analysis (ANA) |
| Legal Advice and Advocacy (LGA) |
| Training, Education, and Awareness (TEA) |
| Cybersecurity Management (MGT) |
| Strategic Planning and Policy (SPP) |
| Cybersecurity Defense Analysis (CDA) |
| Cybersecurity Defense Infrastructure Support (INF) |
| Incident Response (CIR) |
| Vulnerability Assessment and Management (VAM) |
| Threat Analysis (TWA) |
| Exploitation Analysis (EXP) |
| Cyber Operational Planning (OPL) |
| Cyber Operations (OPS) |
| Cyber Investigation (INV) |
| Digital Forensics (FOR) |

**List of Cybersecurity Work Roles that exist at Boston Orthopedics**

|  |
| --- |
| **Work Role** |
| Authorizing Official/Designating Representative |
| Security Control Assessor |
| Software Developer |
| Secure Software Assessor |
| Enterprise Architect |
| Security Architect |
| Research & Development Specialist |
| Systems Requirements Planner |
| System Testing and Evaluation Specialist |
| Information Systems Security Developer |
| Systems Developer |
| Database Administrator |
| Data Analyst |
| Knowledge Manager |
| Technical Support Specialist |
| Network Operations Specialist |
| System Administrator |
| Systems Security Analyst |
| Cyber Legal Advisor |
| Privacy Officer/Privacy Compliance Manager |
| Cyber Instructional Curriculum Developer |
| Cyber Instructor |
| Information Systems Security Manager |
| Communications Security (COMSEC) Manager |
| Cyber Workforce Developer and Manager |
| Cyber Policy and Strategy Planner |
| Cyber Defense Analyst |
| Cyber Defense Infrastructure Support Specialist |
| Cyber Defense Incident Responder |
| Vulnerability Assessment Analyst |
| Threat/Warning Analyst |
| Exploitation Analyst |
| Cyber Intel Planner |
| Cyber Operator |
| Cyber Crime Investigator |
| Cyber Defense Forensics Analyst |

**List of Cybersecurity Tasks that exist at Boston Orthopedics**

|  |
| --- |
| **Task** |
| Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). |
| Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. |
| Establish acceptable limits for the software application, network, or system. |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). |
| Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). |
| Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks. |
| Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. |
| Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. |
| Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers). |
| Establish acceptable limits for the software application, network, or system. |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). |
| Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application. |
| Analyze user needs and software requirements to determine feasibility of design within time and cost constraints. |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. |
| Apply secure code documentation. |
| Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules. |
| Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program. |
| Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces. |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. |
| Apply secure code documentation. |
| Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules. |
| Develop threat model based on customer interviews and requirements. |
| Consult with engineering staff to evaluate interface between hardware and software. |
| Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. |
| Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. |
| Employ secure configuration management processes. |
| Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. |
| Provide advice on project costs, design concepts, or design changes. |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). |
| Analyze candidate architectures, allocate security services, and select security mechanisms. |
| Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. |
| Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. |
| Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. |
| Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET). |
| Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. |
| Employ secure configuration management processes. |
| Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. |
| Review and validate data mining and data warehousing programs, processes, and requirements. |
| Research current technology to understand capabilities of required system or network. |
| Identify cyber capabilities strategies for custom hardware and software development based on mission requirements. |
| Collaborate with stakeholders to identify and/or develop appropriate solutions technology. |
| Design and develop new tools/technologies as related to cybersecurity. |
| Evaluate network infrastructure vulnerabilities to enhance capabilities being developed. |
| Follow software and systems engineering life cycle standards and processes. |
| Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications. |
| Consult with customers to evaluate functional requirements. |
| Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions. |
| Define project scope and objectives based on customer requirements. |
| Develop and document requirements, capabilities, and constraints for design procedures and processes. |
| Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements. |
| Oversee and make recommendations regarding configuration management. |
| Perform needs analysis to determine opportunities for new and improved business process solutions. |
| Prepare use cases to justify the need for specific information technology (IT) solutions. |
| Determine level of assurance of developed capabilities based on test results. |
| Develop test plans to address specifications and requirements. |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). |
| Make recommendations based on test results. |
| Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated. |
| Create auditable evidence of security measures. |
| Validate specifications and requirements for testability. |
| Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. |
| Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications. |
| Assess the effectiveness of cybersecurity measures utilized by system(s). |
| Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile. |
| Build, test, and modify product prototypes using working models or theoretical models. |
| 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). |
| Design and develop cybersecurity or cybersecurity-enabled products. |
| Design hardware, operating systems, and software applications to adequately address cybersecurity requirements. |
| 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. |
| Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. |
| Build, test, and modify product prototypes using working models or theoretical models. |
| Design and develop cybersecurity or cybersecurity-enabled products. |
| Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data. |
| Develop and direct system testing and validation procedures and documentation. |
| Develop architectures or system components consistent with technical specifications. |
| Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. |
| Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable). |
| Analyze and plan for anticipated changes in data capacity requirements. |
| Maintain database management systems software. |
| Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing. |
| Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required. |
| Manage the compilation, cataloging, caching, distribution, and retrieval of data. |
| Monitor and maintain databases to ensure optimal performance. |
| Analyze and define data requirements and specifications. |
| Analyze and plan for anticipated changes in data capacity requirements. |
| Develop data standards, policies, and procedures. |
| Manage the compilation, cataloging, caching, distribution, and retrieval of data. |
| Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. |
| Provide recommendations on new database technologies and architectures. |
| Analyze data sources to provide actionable recommendations. |
| Assess the validity of source data and subsequent findings. |
| Collect metrics and trending data. |
| Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users. |
| Develop an understanding of the needs and requirements of information end-users. |
| Monitor and report the usage of knowledge management assets and resources. |
| Plan and manage the delivery of knowledge management projects. |
| Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information. |
| Lead efforts to promote the organization's use of knowledge management and information sharing. |
| Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files). |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). |
| Troubleshoot system hardware and software. |
| Analyze incident data for emerging trends. |
| Develop and deliver technical training to educate others or meet customer needs. |
| Maintain incident tracking and solution database. |
| Diagnose and resolve customer reported system incidents, problems, and events. |
| Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience. |
| Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling). |
| Develop and implement network backup and recovery procedures. |
| Diagnose network connectivity problem. |
| Implement new system design procedures, test procedures, and quality standards. |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). |
| Install or replace network hubs, routers, and switches. |
| Integrate new systems into existing network architecture. |
| Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing. |
| Comply with organization systems administration standard operating procedures. |
| Implement and enforce local network usage policies and procedures. |
| Manage system/server resources including performance, capacity, availability, serviceability, and recoverability. |
| Ensure all systems security operations and maintenance activities are properly documented and updated as necessary. |
| Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment. |
| Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. |
| Implement specific cybersecurity countermeasures for systems and/or applications. |
| 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. |
| Perform cybersecurity testing of developed applications and/or systems. |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. |
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. |
| Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance. |
| Develop guidelines for implementation. |
| 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. |
| Evaluate the impact of changes to laws, regulations, policies, standards, or procedures. |
| Conduct functional and connectivity testing to ensure continuing operability. |
| Establish a risk management strategy for the organization that includes a determination of risk tolerance. |
| Conduct Privacy Impact Assessments (PIAs) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII). |
| Develop and maintain strategic plans. |
| Evaluate contracts to ensure compliance with funding, legal, and program requirements. |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. |
| Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program. |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. |
| Research current technology to understand capabilities of required system or network. |
| Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction. |
| Conduct learning needs assessments and identify requirements. |
| Create interactive learning exercises to create an effective learning environment. |
| Develop or assist in the development of training policies and protocols for cyber training. |
| Develop the goals and objectives for cyber curriculum. |
| 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. |
| Develop or assist in the development of course assignments. |
| Develop or assist in the development of course evaluations. |
| Develop or assist in the development of grading and proficiency standards. |
| Assist in the development of individual/collective development, training, and/or remediation plans. |
| Develop or assist in the development of learning objectives and goals. |
| Develop or assist in the development of on-the-job training materials or programs. |
| Develop or assist in the development of written tests for measuring and assessing learner proficiency. |
| Conduct learning needs assessments and identify requirements. |
| Develop or assist in the development of training policies and protocols for cyber training. |
| Develop the goals and objectives for cyber curriculum. |
| Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications. |
| Consult with customers to evaluate functional requirements. |
| Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions. |
| Define project scope and objectives based on customer requirements. |
| Develop and document requirements, capabilities, and constraints for design procedures and processes. |
| Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements. |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. |
| Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. |
| Ensure that security improvement actions are evaluated, validated, and implemented as required. |
| Develop policy, programs, and guidelines for implementation. |
| Establish and maintain communication channels with stakeholders. |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. |
| Identify organizational policy stakeholders. |
| Review existing and proposed policies with stakeholders. |
| Serve on agency and interagency policy boards. |
| Develop policy, programs, and guidelines for implementation. |
| Establish and maintain communication channels with stakeholders. |
| Review existing and proposed policies with stakeholders. |
| Serve on agency and interagency policy boards. |
| Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. |
| Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. |
| 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. |
| 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. |
| Perform cyber defense trend analysis and reporting. |
| 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. |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. |
| Plan and recommend modifications or adjustments based on exercise results or system environment. |
| Provide daily summary reports of network events and activity relevant to cyber defense practices. |
| Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. |
| Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. |
| Build, install, configure, and test dedicated cyber defense hardware. |
| Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure. |
| Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s). |
| Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems). |
| Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization). |
| Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. |
| Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. |
| Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security. |
| Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. |
| Perform cyber defense trend analysis and reporting. |
| Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. |
| Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. |
| Conduct and/or support authorized penetration testing on enterprise network assets. |
| Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. |
| Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. |
| Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. |
| Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews). |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. |
| Assist in the identification of intelligence collection shortfalls. |
| Brief threat and/or target current situations. |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. |
| Conduct in-depth research and analysis. |
| Conduct nodal analysis. |
| Develop information requirements necessary for answering priority information requests. |
| Evaluate threat decision-making processes. |
| Identify threats to Blue Force vulnerabilities. |
| Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements. |
| Apply and obey applicable statutes, laws, regulations and policies. |
| Perform analysis for target infrastructure exploitation activities. |
| Collaborate with other internal and external partner organizations on target access and operational issues. |
| Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers. |
| Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities. |
| Incorporate cyber operations and communications security support plans into organization objectives. |
| Identify cyber intelligence gaps and shortfalls for cyber operational planning. |
| Integrate cyber planning/targeting efforts with other organizations. |
| Interpret environment preparations assessments to determine a course of action. |
| Issue requests for information. |
| Maintain relationships with internal and external partners involved in cyber planning or related areas. |
| Maintain situational awareness of cyber-related intelligence requirements and associated tasking. |
| Maintain situational awareness of partner capabilities and activities. |
| Maintain situational awareness to determine if changes to the operating environment require review of the plan. |
| Conduct exploitation of wireless computer and digital networks. |
| Conduct network scouting and vulnerability analyses of systems within a network. |
| Conduct on-net activities to control and exfiltrate data from deployed technologies. |
| Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies. |
| Conduct open source data collection via various online tools. |
| Conduct survey of computer and digital networks. |
| Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers). |
| Detect exploits against targeted networks and hosts and react accordingly. |
| Develop new techniques for gaining and keeping access to target systems. |
| Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems. |
| Exploit network devices, security devices, and/or terminals or environments using various methods or tools. |
| Facilitate access enabling by physical and/or wireless means. |
| Identify potential points of strength and vulnerability within a network. |
| Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation. |
| Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks. |
| Provide criminal investigative support to trial counsel during the judicial process. |
| Analyze computer-generated threats for counter intelligence or criminal activity. |
| Gather and preserve evidence used on the prosecution of computer crimes. |
| 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. |
| 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. |
| Decrypt seized data using technical means. |
| Provide technical summary of findings in accordance with established reporting procedures. |
| Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence. |
| Examine recovered data for information of relevance to the issue at hand. |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. |
| 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. |
| Perform file signature analysis. |

**Comparison of NCWF recommended cybersecurity specialty areas with Boston Orthopedics existing cybersecurity specialty areas.**

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

**Comparison of NCWF recommended cybersecurity Tasks with Boston Orthopedics existing cybersecurity specialty areas.**

|  |  |  |
| --- | --- | --- |
| **Work Role** | **Tasks** | **Status** |
| Authorizing  Official/Designating  Representative | Manage and Approve Accreditation Packages (e.g., ISO/IEC 15026-2). | Present |
| Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. | Present |
| Establish acceptable limits for the software application, network, or system. | Present |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). | Present |
| Security control Assessor | Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). | Present |
| Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks. | Present |
| Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. | Present |
| Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. | Present |
| Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centres). | Present |
| Establish acceptable limits for the software application, network, or system. | Absent |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). | Present |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. | Present |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. | Present |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Present |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Present |
| Verify and update security documentation reflecting the application/system security design features. | Present |
| Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. | Present |
| Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. | Present |
| Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals. | Present |
| Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. | Present |
| Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. | Absent |
| Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Assess the effectiveness of security controls. | Absent |
| Assess all the configuration management (change configuration/release management) processes. | Absent |
| Software Developer  (DEV) | Analyse information to determine, recommend, and plan the development of a new application or modification of an existing application. | Present |
| Analyse user needs and software requirements to determine feasibility of design within time and cost constraints. | Absent |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. | Present |
| Apply secure code documentation. | Absent |
| Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules. | Present |
| Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program. | Absent |
| Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces. | Absent |
| Consult with engineering staff to evaluate interface between hardware and software. | Present |
| Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced. | Present |
| Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design. | Absent |
| Develop secure code and error handling. | Absent |
| Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. | Absent |
| Identify basic common coding flaws at a high level. | Absent |
| Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. | Absent |
| Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life. | Absent |
| Perform integrated quality assurance testing for security functionality and resiliency attack. | Absent |
| Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities. | Present |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Present |
| Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language. | Absent |
| Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. | Present |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Present |
| Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modelling, and defining any specific security criteria. | Present |
| Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements. | Present |
| Identify and leverage the enterprise-wide version control system while designing and developing secure applications. | Present |
| Consult with customers about software system design and maintenance. | Absent |
| Direct software programming and development of documentation. | Absent |
| Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Absent |
| Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | Present |
| Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate. | Present |
| Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct. | Present |
| Develop software system testing and validation procedures, programming, and documentation. | Present |
| Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance. | Present |
| Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities. | Present |
| Determine and document software patches or the extent of releases that would leave software vulnerable. | Present |
| Secure Software Assessor | Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. | Present |
| Apply secure code documentation. | Present |
| Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules. | Present |
| Develop threat model based on customer interviews and requirements. | Present |
| Consult with engineering staff to evaluate interface between hardware and software. | Present |
| Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. | Present |
| Identify basic common coding flaws at a high level. | Present |
| Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. | Present |
| Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life. | Absent |
| Perform integrated quality assurance testing for security functionality and resiliency attack. | Present |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Present |
| Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. | Present |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Present |
| Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modelling, and defining any specific security criteria. | Present |
| Perform penetration testing as required for new or updated applications. | Present |
| Consult with customers about software system design and maintenance. | Present |
| Direct software programming and development of documentation. | Absent |
| Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Absent |
| Analyse and provide information to stakeholders that will support the development of security application or modification of an existing security application. | Absent |
| Analyse security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates. | Absent |
| Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct. | Absent |
| Develop secure software testing and validation procedures. | Present |
| Develop system testing and validation procedures, programming, and documentation. | Present |
| Develop enterprise architecture or system components required to meet user needs. | Present |
| Document and update as necessary all definition and architecture activities. | Present |
| Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities. | Absent |
| Determine and document software patches or the extent of releases that would leave software vulnerable. | Absent |
| Enterprise Architect | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | Absent |
| Employ secure configuration management processes. | Absent |
| Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. | Absent |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. | Absent |
| Provide advice on project costs, design concepts, or design changes. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Absent |
| Analyse candidate architectures, allocate security services, and select security mechanisms. | Absent |
| Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | Absent |
| Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. | Absent |
| Write detailed functional specifications that document the architecture development process. | Absent |
| Analyse user needs and requirements to plan architecture. | Absent |
| Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. | Absent |
| Develop enterprise architecture or system components required to meet user needs. | Absent |
| Document and update as necessary all definition and architecture activities. | Absent |
| Integrate results regarding the identification of gaps in security architecture. | Absent |
| Plan implementation strategy to ensure that enterprise components can be integrated and aligned. | Absent |
| Translate proposed capabilities into technical requirements. | Absent |
| Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture. | Absent |
| Integrate key management functions as related to cyberspace. | Absent |
| Security architect | Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. | Absent |
| Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | Absent |
| Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET). | Absent |
| Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. | Absent |
| Employ secure configuration management processes. | Absent |
| Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. | Absent |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. | Absent |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. | Absent |
| Provide advice on project costs, design concepts, or design changes. | Absent |
| Provide input on security requirements to be included in statements of work and other appropriate procurement documents. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Absent |
| Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. | Absent |
| Analyse candidate architectures, allocate security services, and select security mechanisms. | Absent |
| Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | Absent |
| Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. | Absent |
| Write detailed functional specifications that document the architecture development process. | Absent |
| Analyse user needs and requirements to plan architecture. | Absent |
| Develop enterprise architecture or system components required to meet user needs. | Absent |
| Document and update as necessary all definition and architecture activities. | Absent |
| Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. | Absent |
| Translate proposed capabilities into technical requirements. | Absent |
| Assess and design security management functions as related to cyberspace. | Absent |
| Research And Development Specialist | Review and validate data mining and data warehousing programs, processes, and requirements. | Absent |
| Research current technology to understand capabilities of required system or network. | Absent |
| Identify cyber capabilities strategies for custom hardware and software development based on mission requirements. | Absent |
| Collaborate with stakeholders to identify and/or develop appropriate solutions technology. | Absent |
| Design and develop new tools/technologies as related to cybersecurity. | Absent |
| Evaluate network infrastructure vulnerabilities to enhance capabilities being developed. | Absent |
| Follow software and systems engineering life cycle standards and processes. | Absent |
| Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases. | Absent |
| Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities. | Absent |
| Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. | Absent |
| Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce. | Absent |
| Research and evaluate available technologies and standards to meet customer requirements. | Absent |
| Systems Requirements Planner | Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications. | Present |
| Consult with customers to evaluate functional requirements. | Present |
| Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions. | Present |
| Define project scope and objectives based on customer requirements. | Present |
| Develop and document requirements, capabilities, and constraints for design procedures and processes. | Present |
| Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements. | Present |
| Oversee and make recommendations regarding configuration management. | Absent |
| Perform needs analysis to determine opportunities for new and improved business process solutions. | Absent |
| Prepare use cases to justify the need for specific information technology (IT) solutions. | Absent |
| Translate functional requirements into technical solutions. | Absent |
| Develop and document supply chain risks for critical system elements, as appropriate. | Present |
| Develop and document User Experience (UX) requirements including information architecture and user interface requirements. | Present |
| Design and document quality standards. | Present |
| Document a system's purpose and preliminary system security concept of operations. | Present |
| Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware). | Present |
| Define baseline security requirements in accordance with applicable guidelines. | Absent |
| Develop cost estimates for new or modified system(s). | Absent |
| Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements. | Absent |
| System Testing and Evaluation Specialist | Determine level of assurance of developed capabilities based on test results. | Present |
| Develop test plans to address specifications and requirements. | Present |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Present |
| Make recommendations based on test results. | Present |
| Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated. | Present |
| Create auditable evidence of security measures. | Present |
| Validate specifications and requirements for testability. | Present |
| Analyse the results of software, hardware, or interoperability testing. | Present |
| Perform developmental testing on systems under development. | Present |
| Perform interoperability testing on systems exchanging electronic information with other systems. | Present |
| Perform operational testing. | Present |
| Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements. | Present |
| Record and manage test data. | Present |
| Information Systems Security Developer | Analyse design constraints, Analyse trade-offs and detailed system and security design, and consider life cycle support. | Absent |
| Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications. | Absent |
| Assess the effectiveness of cybersecurity measures utilized by system(s). | Absent |
| Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile. | Absent |
| Build, test, and modify product prototypes using working models or theoretical models. | Absent |
| Conduct Privacy Impact Assessments (PIAs) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII). | Absent |
| Design and develop cybersecurity or cybersecurity-enabled products. | Absent |
| Design hardware, operating systems, and software applications to adequately address cybersecurity requirements. | Absent |
| Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data. | Absent |
| Develop and direct system testing and validation procedures and documentation. | Absent |
| Develop detailed security design documentation for component and interface specifications to support system design and development. | Absent |
| Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | Absent |
| Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed. | Absent |
| Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications. | Absent |
| Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements. | Absent |
| Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable). | Absent |
| Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability. | Absent |
| Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements. | Absent |
| Implement security designs for new or existing system(s). | Absent |
| Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts). | Absent |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Absent |
| Provide guidelines for implementing developed systems to customers or installation teams. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Absent |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Absent |
| Provide support to security/certification test and evaluation activities. | Absent |
| Utilize models and simulations to Analyse or predict system performance under different operating conditions. | Absent |
| Design and develop key management functions (as related to cybersecurity). | Absent |
| Analyse user needs and requirements to plan and conduct system security development. | Absent |
| Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information). | Absent |
| Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. | Absent |
| Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment. | Absent |
| Employ configuration management processes. | Absent |
| Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. | Absent |
| Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation. | Absent |
| Design to security requirements to ensure requirements are met for all systems and/or applications. | Absent |
| Develop mitigation strategies to address cost, schedule, performance, and security risks. | Absent |
| Perform an information security risk assessment. | Absent |
| Perform security reviews and identify security gaps in architecture. | Absent |
| Provide input to implementation plans and standard operating procedures as they relate to information systems security. | Absent |
| Trace system requirements to design components and perform gap analysis. | Absent |
| Verify stability, interoperability, portability, and/or scalability of system architecture. | Absent |
| Systems Developer | Analyse design constraints, Analyse trade-offs and detailed system and security design, and consider life cycle support. | Absent |
| Build, test, and modify product prototypes using working models or theoretical models. | Absent |
| Design and develop cybersecurity or cybersecurity-enabled products. | Absent |
| Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data. | Absent |
| Develop and direct system testing and validation procedures and documentation. | Absent |
| Develop architectures or system components consistent with technical specifications. | Absent |
| Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | Absent |
| Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable). | Absent |
| Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability. | Absent |
| Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements. | Absent |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Absent |
| Provide guidelines for implementing developed systems to customers or installation teams. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Absent |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Absent |
| Utilize models and simulations to Analyse or predict system performance under different operating conditions. | Absent |
| Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment. | Absent |
| Employ configuration management processes. | Absent |
| Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements. | Absent |
| Design and develop system administration and management functionality for privileged access users. | Absent |
| Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. | Absent |
| Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle). | Absent |
| Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary. | Absent |
| Design hardware, operating systems, and software applications to adequately address requirements. | Absent |
| Design to security requirements to ensure requirements are met for all systems and/or applications. | Absent |
| Develop detailed design documentation for component and interface specifications to support system design and development. | Absent |
| Develop mitigation strategies to address cost, schedule, performance, and security risks. | Absent |
| Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements. | Absent |
| Implement designs for new or existing system(s). | Absent |
| Perform security reviews and identify security gaps in architecture. | Absent |
| Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials | Absent |
| Provide support to test and evaluation activities. | Absent |
| Trace system requirements to design components and perform gap analysis. | Absent |
| Verify stability, interoperability, portability, and/or scalability of system architecture. | Absent |
| Analyse user needs and requirements to plan and conduct system development. | Absent |
| Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations. | Absent |
| Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information). | Absent |
| Database Administrator | Analyse and plan for anticipated changes in data capacity requirements. | Present |
| Maintain database management systems software. | Present |
| Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing. | Present |
| Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required. | Present |
| Manage the compilation, cataloguing, caching, distribution, and retrieval of data. | Present |
| Monitor and maintain databases to ensure optimal performance. | Present |
| Perform backup and recovery of databases to ensure data integrity. | Present |
| Provide recommendations on new database technologies and architectures. | Absent |
| Performs configuration management, problem management, capacity management, and financial management for databases and data management systems. | Absent |
| Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems. | Absent |
| Maintain assured message delivery systems. | Absent |
| Implement data management standards, requirements, and specifications. | Present |
| Implement data mining and data warehousing applications. | Present |
| Install and configure database management systems and software. | Present |
| Data Analyst | Analyse and define data requirements and specifications. | Absent |
| Analyse and plan for anticipated changes in data capacity requirements. | Absent |
| Develop data standards, policies, and procedures. | Absent |
| Manage the compilation, cataloguing, caching, distribution, and retrieval of data. | Absent |
| Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | Absent |
| Provide recommendations on new database technologies and architectures. | Absent |
| Analyse data sources to provide actionable recommendations. | Absent |
| Assess the validity of source data and subsequent findings. | Absent |
| Collect metrics and trending data. | Absent |
| Conduct hypothesis testing using statistical processes. | Absent |
| Confer with systems analysts, engineers, programmers, and others to design application. | Absent |
| Develop and facilitate data-gathering methods. | Absent |
| Develop strategic insights from large data sets. | Absent |
| Present technical information to technical and nontechnical audiences. | Absent |
| Present data in creative formats. | Absent |
| Program custom algorithms. | Absent |
| Provide actionable recommendations to critical stakeholders based on data analysis and findings. | Absent |
| Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method. | Absent |
| Effectively allocate storage capacity in the design of data management systems. | Absent |
| Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data). | Absent |
| Utilize different programming languages to write code, open files, read files, and write output to different files. | Absent |
| Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line). | Absent |
| Develop and implement data mining and data warehousing programs. | Absent |
| Knowledge Manager | Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users. | Absent |
| Develop an understanding of the needs and requirements of information end-users. | Absent |
| Monitor and report the usage of knowledge management assets and resources. | Absent |
| Plan and manage the delivery of knowledge management projects. | Absent |
| Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information. | Absent |
| Lead efforts to promote the organization's use of knowledge management and information sharing. | Absent |
| Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files). | Absent |
| Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization’s intellectual capital. | Absent |
| Promote knowledge sharing between information owners/users through an organization’s operational processes and systems. | Absent |
| Technical Support Specialist | Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Present |
| Troubleshoot system hardware and software. | Present |
| Analyse incident data for emerging trends. | Present |
| Develop and deliver technical training to educate others or meet customer needs. | Present |
| Maintain incident tracking and solution database. | Present |
| Diagnose and resolve customer reported system incidents, problems, and events. | Present |
| Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience. | Present |
| Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards. | Present |
| Administer accounts, network rights, and access to systems and equipment. | Present |
| Perform asset management/inventory of information technology (IT) resources. | Present |
| Monitor and report client-level computer system performance. | Present |
| Develop a trend analysis and impact report. | Present |
| Network Operations Specialist | Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunnelling). | Present |
| Develop and implement network backup and recovery procedures. | Present |
| Diagnose network connectivity problem. | Present |
| Implement new system design procedures, test procedures, and quality standards. | Present |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Present |
| Install or replace network hubs, routers, and switches. | Present |
| Integrate new systems into existing network architecture. | Present |
| Monitor network capacity and performance. | Present |
| Patch network vulnerabilities to ensure that information is safeguarded against outside parties. | Present |
| Provide feedback on network requirements, including network architecture and infrastructure. | Present |
| Test and maintain network infrastructure including software and hardware devices. | Present |
| System Administrator | Conduct functional and connectivity testing to ensure continuing operability. | Present |
| Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs. | Present |
| Develop and document systems administration standard operating procedures. | Present |
| Maintain baseline system security according to organizational policies. | Absent |
| Manage accounts, network rights, and access to systems and equipment. | Present |
| Plan, execute, and verify data redundancy and system recovery procedures. | Present |
| Provide ongoing optimization and problem-solving support. | Present |
| Install, update, and troubleshoot systems/servers. | Present |
| Check system hardware availability, functionality, integrity, and efficiency. | Present |
| Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing. | Present |
| Comply with organization systems administration standard operating procedures. | Present |
| Implement and enforce local network usage policies and procedures. | Present |
| Manage system/server resources including performance, capacity, availability, serviceability, and recoverability. | Present |
| Monitor and maintain system/server configuration. | Present |
| Oversee installation, implementation, configuration, and support of system components. | Present |
| Diagnose faulty system/server hardware. | Present |
| Perform repairs on faulty system/server hardware. | Present |
| Troubleshoot hardware/software interface and interoperability problems. | Present |
| System Security Analyst | Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications. | Present |
| Apply security policies to meet security objectives of the system. | Present |
| Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | Present |
| Ensure all systems security operations and maintenance activities are properly documented and updated as necessary. | Present |
| Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment. | Present |
| Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. | Present |
| Implement specific cybersecurity countermeasures for systems and/or applications. | Present |
| 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. | Present |
| Perform cybersecurity testing of developed applications and/or systems. | Present |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. | Absent |
| Plan and recommend modifications or adjustments based on exercise results or system environment. | Absent |
| Properly document all systems security implementation, operations, and maintenance activities and update as necessary. | Absent |
| Provide cybersecurity guidance to leadership. | Present |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Absent |
| Verify and update security documentation reflecting the application/system security design features. | Absent |
| Assess the effectiveness of security controls. | Absent |
| Assess all the configuration management (change configuration/release management) processes. | Absent |
| Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements. | Absent |
| Analyse and report organizational security posture trends. | Absent |
| Analyse and report system security posture trends. | Absent |
| Assess adequate access controls based on principles of least privilege and need-to-know. | Absent |
| Ensure the execution of disaster recovery and continuity of operations. | Absent |
| Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed. | Absent |
| Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | Absent |
| Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment. | Absent |
| Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative. | Absent |
| Assess and monitor cybersecurity related to system implementation and testing practices. | Absent |
| Verify minimum security requirements are in place for all applications. | Absent |
| Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. | Absent |
| Work with stakeholders to resolve computer security incidents and vulnerability compliance. | Present |
| Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. | Present |
| Cyber Legal Advisor | Advocate organization's official position in legal and legislative proceedings. | Absent |
| Evaluate contracts to ensure compliance with funding, legal, and program requirements. | Absent |
| Evaluate the effectiveness of laws, regulations, policies, standards, or procedures. | Absent |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. | Absent |
| Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance. | Absent |
| Develop guidelines for implementation. | Absent |
| Provide legal analysis and decisions to inspectors general, privacy officers, oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements. | Absent |
| Evaluate the impact of changes to laws, regulations, policies, standards, or procedures. | Absent |
| Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. | Absent |
| Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures. | Absent |
| Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery). | Absent |
| Privacy Officer/Privacy Compliance Manager | Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. | Absent |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| Conduct functional and connectivity testing to ensure continuing operability. | Absent |
| Establish a risk management strategy for the organization that includes a determination of risk tolerance. | Absent |
| Conduct Privacy Impact Assessments (PIAs) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII). | Absent |
| Develop and maintain strategic plans. | Absent |
| Evaluate contracts to ensure compliance with funding, legal, and program requirements. | Absent |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Absent |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. | Absent |
| Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program. | Absent |
| Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. | Absent |
| Present technical information to technical and nontechnical audiences. | Absent |
| Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. | Absent |
| Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. | Absent |
| Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations. | Absent |
| Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements. | Absent |
| Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner. | Absent |
| Liaise with regulatory and accrediting bodies. | Absent |
| Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues. | Absent |
| Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance. | Absent |
| Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required. | Absent |
| Work with business teams and senior management to ensure awareness of “best practices” on privacy and data security issues. | Absent |
| Work with organization senior management to establish an organization-wide Privacy Oversight Committee | Absent |
| Serve in a leadership role for Privacy Oversight Committee activities | Absent |
| Collaborate on cyber privacy and security policies and procedures | Absent |
| Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation | Absent |
| Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations | Absent |
| Provide strategic guidance to corporate officers regarding information resources and technology | Absent |
| Assist the Security Officer with the development and implementation of an information infrastructure | Absent |
| Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations. | Absent |
| Work cooperatively with applicable organization units in overseeing consumer information access rights | Absent |
| Serve as the information privacy liaison for users of technology systems | Absent |
| Act as a liaison to the information systems department | Absent |
| Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations | Absent |
| Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties | Absent |
| Conduct on-going privacy training and awareness activities | Absent |
| Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security | Absent |
| Work with organization administration, legal counsel and other related parties to represent the organization’s information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard. | Absent |
| Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee | Absent |
| Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data | Absent |
| Provide leadership for the organization’s privacy program | Absent |
| Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization | Absent |
| Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization’s workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable | Absent |
| Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures | Absent |
| Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices | Absent |
| Develop and coordinate a risk management and compliance framework for privacy | Absent |
| Undertake a comprehensive review of the company’s data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies. | Absent |
| Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations | Absent |
| Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization’s privacy policies and procedures | Absent |
| Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity | Absent |
| Provide leadership in the planning, design and evaluation of privacy and security related projects | Absent |
| Establish an internal privacy audit program | Absent |
| Periodically revise the privacy program considering changes in laws, regulatory or company policy | Absent |
| Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel | Absent |
| Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information | Absent |
| Monitor systems development and operations for security and privacy compliance | Absent |
| Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected | Absent |
| Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization’s other compliance and operational assessment functions | Absent |
| Review all system-related information security plans to ensure alignment between security and privacy practices | Absent |
| Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization’s policies, procedures and legal requirements | Absent |
| Account for and administer individual requests for release or disclosure of personal and/or protected information | Absent |
| Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements | Absent |
| Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed | Absent |
| Act as, or work with, counsel relating to business partner contracts | Absent |
| Mitigate effects of a use or disclosure of personal information by employees or business partners | Absent |
| Develop and apply corrective action procedures | Absent |
| Administer action on all complaints concerning the organization’s privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel | Absent |
| Support the organization’s privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations | Absent |
| Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations | Absent |
| Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units | Absent |
| Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices | Absent |
| Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations | Absent |
| Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials | Absent |
| Cyber Instructional Curriculum Developer | Support the design and execution of exercise scenarios. | Absent |
| Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. | Absent |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. | Absent |
| Research current technology to understand capabilities of required system or network. | Absent |
| Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction. | Absent |
| Conduct learning needs assessments and identify requirements. | Absent |
| Create interactive learning exercises to create an effective learning environment. | Absent |
| Develop or assist in the development of training policies and protocols for cyber training. | Absent |
| Develop the goals and objectives for cyber curriculum. | Absent |
| Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers. | Absent |
| Correlate training and learning to business or mission requirements. | Absent |
| Create training courses tailored to the audience and physical environment. | Absent |
| Design training curriculum and course content based on requirements. | Absent |
| Participate in development of training curriculum and course content. | Absent |
| Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions). | Absent |
| Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). | Absent |
| Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations. | Absent |
| Cyber Instructor | Conduct interactive training exercises to create an effective learning environment. | Absent |
| Develop new or identify existing awareness and training materials that are appropriate for intended audiences. | Absent |
| Evaluate the effectiveness and comprehensiveness of existing training programs. | Absent |
| Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions). | Absent |
| Support the design and execution of exercise scenarios. | Absent |
| Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. | Absent |
| Develop or assist in the development of computer-based training modules or classes. | Absent |
| Develop or assist in the development of course assignments. | Absent |
| Develop or assist in the development of course evaluations. | Absent |
| Develop or assist in the development of grading and proficiency standards. | Absent |
| Assist in the development of individual/collective development, training, and/or remediation plans. | Absent |
| Develop or assist in the development of learning objectives and goals. | Absent |
| Develop or assist in the development of on-the-job training materials or programs. | Absent |
| Develop or assist in the development of written tests for measuring and assessing learner proficiency. | Absent |
| Conduct learning needs assessments and identify requirements. | Absent |
| Develop or assist in the development of training policies and protocols for cyber training. | Absent |
| Develop the goals and objectives for cyber curriculum. | Absent |
| Present technical information to technical and nontechnical audiences. | Absent |
| Present data in creative formats. | Absent |
| Write and publish after action reviews. | Absent |
| Deliver training courses tailored to the audience and physical/virtual environments. | Absent |
| Apply concepts, procedures, software, equipment, and/or technology applications to students. | Absent |
| Design training curriculum and course content based on requirements. | Absent |
| Participate in development of training curriculum and course content. | Absent |
| Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness. | Absent |
| Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment. | Absent |
| Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses). | Absent |
| Recommend revisions to curriculum and course content based on feedback from previous training sessions. | Absent |
| Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). | Absent |
| Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations. | Absent |
| Information Systems Security Manager | Manage the monitoring of information security data sources to maintain organizational situational awareness.  Manage the publishing of Computer Network Defence guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. | Present |
| Manage the publishing of Computer Network Defence guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. | Present |
| Manage threat or target analysis of cyber defence information and production of threat information within the enterprise. | Present |
| Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. | Present |
| Oversee the information security training and awareness program. | Present |
| Participate in an information security risk assessment during the Security Assessment and Authorization process. | Present |
| Participate in the development or modification of the computer environment cybersecurity program plans and requirements. | Present |
| Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations. | Present |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | Present |
| 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 |
| Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents. | Present |
| Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters. | Present |
| Recognize a possible security violation and take appropriate action to report the incident, as required. | Present |
| Recommend resource allocations required to securely operate and maintain an organization’s cybersecurity requirements. | Present |
| Recommend policy and coordinate review and approval.  Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Present |
| Track audit findings and recommendations to ensure that appropriate mitigation actions are taken. | Present |
| Use federal and organization-specific published documents to manage operations of their computing environment system(s). | Present |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. | Present |
| Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. | Present |
| Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. | Present |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Present |
| Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. | Present |
| Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. | Present |
| Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals. | Present |
| Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). | Present |
| Participate in the acquisition process as necessary, following appropriate supply chain risk management practices. | Present |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Present |
| Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance. | Present |
| Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary. | Present |
| Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate. | Present |
| Communications Security (COMSEC) Manager | Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. | Present |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Present |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Present |
| Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. | Present |
| Ensure that security improvement actions are evaluated, validated, and implemented as required. | Present |
| Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy. | Present |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Present |
| Recognize a possible security violation and take appropriate action to report the incident, as required. | Present |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Present |
| Cyber Workforce Developer and Manager | Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. | Absent |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Absent |
| Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. | Absent |
| Develop policy, programs, and guidelines for implementation. | Absent |
| Establish and maintain communication channels with stakeholders. | Absent |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Absent |
| Identify organizational policy stakeholders. | Absent |
| Review existing and proposed policies with stakeholders. | Absent |
| Serve on agency and interagency policy boards. | Absent |
| Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. | Absent |
| Conduct learning needs assessments and identify requirements. | Absent |
| Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards. | Absent |
| Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. | Absent |
| Develop and implement standardized position descriptions based on established cyber work roles. | Absent |
| Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies. | Absent |
| Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers. | Absent |
| Develop or assist in the development of training policies and protocols for cyber training. | Absent |
| Ensure that cyber career fields are managed in accordance with organizational HR policies and directives. | Absent |
| Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. | Absent |
| Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel. | Absent |
| Establish and oversee waiver processes for cyber career field entry and training qualification requirements. | Absent |
| Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields. | Absent |
| Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements. | Absent |
| Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements. | Absent |
| Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. | Absent |
| Review and apply cyber career field qualification standards. | Absent |
| Review and apply organizational policies related to or influencing the cyber workforce. | Absent |
| Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. | Absent |
| Support integration of qualified cyber workforce personnel into information systems life cycle development processes. | Absent |
| Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. | Absent |
| Analyse organizational cyber policy. | Absent |
| Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. | Absent |
| Correlate training and learning to business or mission requirements. | Absent |
| Define and integrate current and future mission environments. | Absent |
| Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan. | Absent |
| Draft, staff, and publish cyber policy. | Absent |
| Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training). | Absent |
| Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. | Absent |
| Seek consensus on proposed policy changes from stakeholders. | Absent |
| Provide policy guidance to cyber management, staff, and users. | Absent |
| Review, conduct, or participate in audits of cyber programs and projects. | Absent |
| Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). | Absent |
| Support the CIO in the formulation of cyber-related policies. | Absent |
| Review and approve a supply chain security/risk management policy. | Absent |
| Cyber Policy and Strategy Planner | Develop policy, programs, and guidelines for implementation. | Absent |
| Establish and maintain communication channels with stakeholders. | Absent |
| Review existing and proposed policies with stakeholders. | Absent |
| Serve on agency and interagency policy boards. | Absent |
| Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. | Absent |
| Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. | Absent |
| Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. | Absent |
| Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. | Absent |
| Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. | Absent |
| Analyse organizational cyber policy. | Absent |
| Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. | Absent |
| Define and integrate current and future mission environments. | Absent |
| Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan. | Absent |
| Draft, staff, and publish cyber policy. | Absent |
| Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. | Absent |
| Seek consensus on proposed policy changes from stakeholders. | Absent |
| Provide policy guidance to cyber management, staff, and users. | Absent |
| Review, conduct, or participate in audits of cyber programs and projects. | Absent |
| Support the CIO in the formulation of cyber-related policies. | Absent |
| Executive Cyber Leadership | Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. | Absent |
| Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program. | Absent |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| Advocate organization's official position in legal and legislative proceedings. | Absent |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Absent |
| Develop and maintain strategic plans. | Absent |
| Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defence information. | Absent |
| Lead and align information technology (IT) security priorities with the security strategy. | Absent |
| Lead and oversee information security budget, staffing, and contracting. | Absent |
| Manage the publishing of Computer Network Defence guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. | Absent |
| Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. | Absent |
| Recommend policy and coordinate review and approval. | Absent |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Absent |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Absent |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. | Absent |
| Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. | Absent |
| Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. | Absent |
| Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. | Absent |
| Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate. | Absent |
| Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Absent |
| Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. | Absent |
| Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. | Absent |
| Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan. | Absent |
| Perform an information security risk assessment. | Absent |
| Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| Collaborate on cyber privacy and security policies and procedures | Absent |
| Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation | Absent |
| Appoint and guide a team of IT security experts. | Absent |
| Collaborate with key stakeholders to establish a cybersecurity risk management program. | Absent |
| Program Manager | Develop and maintain strategic plans. | Present |
| Develop methods to monitor and measure risk, compliance, and assurance efforts. | Present |
| Perform needs analysis to determine opportunities for new and improved business process solutions. | Present |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | Present |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| Review or conduct audits of information technology (IT) programs and projects. | Present |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Present |
| Develop and document supply chain risks for critical system elements, as appropriate. | Present |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Present |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Present |
| Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully. | Present |
| Coordinate and manage the overall service provided to a customer end-to-end. | Present |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Absent |
| Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). | Absent |
| Participate in the acquisition process as necessary. | Absent |
| Conduct import/export reviews for acquiring systems and software. | Present |
| Develop supply chain, system, network, performance, and cybersecurity requirements. | Present |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Present |
| Identify and address cyber workforce planning and management issues (e.g., recruitment, retention, and training). | Absent |
| Lead and oversee budget, staffing, and contracting. | Absent |
| Draft and publish supply chain security and risk management documents. | Absent |
| IT Project Manager | Develop methods to monitor and measure risk, compliance, and assurance efforts. | Present |
| Perform needs analysis to determine opportunities for new and improved business process solutions. | Present |
| Provide advice on project costs, design concepts, or design changes. | Present |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | Present |
| Provide ongoing optimization and problem-solving support. | Absent |
| Provide recommendations for possible improvements and upgrades. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Absent |
| Develop and document supply chain risks for critical system elements, as appropriate. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully. | Absent |
| Coordinate and manage the overall service provided to a customer end-to-end. | Absent |
| Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service. | Absent |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Present |
| Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). | Present |
| Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. | Present |
| Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives. | Present |
| Participate in the acquisition process as necessary. | Present |
| Conduct import/export reviews for acquiring systems and software. | Present |
| Develop supply chain, system, network, performance, and cybersecurity requirements. | Present |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Present |
| Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training). | Present |
| Lead and oversee budget, staffing, and contracting. | Present |
| Draft and publish supply chain security and risk management documents. | Present |
| Product Support Manager | Develop methods to monitor and measure risk, compliance, and assurance efforts. | Absent |
| Perform needs analysis to determine opportunities for new and improved business process solutions. | Absent |
| Provide advice on project costs, design concepts, or design changes. | Absent |
| Provide input to implementation plans and standard operating procedures. | Absent |
| Provide ongoing optimization and problem-solving support. | Absent |
| Provide recommendations for possible improvements and upgrades. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Absent |
| Develop and document supply chain risks for critical system elements, as appropriate. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Absent |
| Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully. | Absent |
| Coordinate and manage the overall service provided to a customer end-to-end. | Absent |
| Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service. | Absent |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Absent |
| Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. | Absent |
| Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives. | Absent |
| Conduct import/export reviews for acquiring systems and software. | Absent |
| Develop supply chain, system, network, performance, and cybersecurity requirements. | Absent |
| Lead and oversee budget, staffing, and contracting. | Absent |
| Provide enterprise cybersecurity and supply chain risk management guidance. | Absent |
| Draft and publish supply chain security and risk management documents. | Absent |
| Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities. | Absent |
| IT Investment/Portfolio Manager | Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Absent |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Absent |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Absent |
| Lead and oversee budget, staffing, and contracting. | Absent |
| Draft and publish supply chain security and risk management documents. | Absent |
| IT Program Auditor | Develop methods to monitor and measure risk, compliance, and assurance efforts. | Absent |
| Provide ongoing optimization and problem-solving support. | Absent |
| Provide recommendations for possible improvements and upgrades. | Absent |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Absent |
| Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. | Absent |
| Conduct import/export reviews for acquiring systems and software. | Absent |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Absent |
| Cyber Defence Analyst | Develop content for cyber defence tools. | Absent |
| Characterize and Analyse network traffic to identify anomalous activity and potential threats to network resources. | Absent |
| Coordinate with enterprise-wide cyber defence staff to validate network alerts. | Absent |
| Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. | Absent |
| Document and escalate incidents (including event’s history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment. | Absent |
| Perform cyber defence trend analysis and reporting. | Absent |
| Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | Absent |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. | Absent |
| Plan and recommend modifications or adjustments based on exercise results or system environment. | Absent |
| Provide daily summary reports of network events and activity relevant to cyber defence practices. | Absent |
| Receive and Analyse network alerts from various sources within the enterprise and determine possible causes of such alerts. | Absent |
| Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. | Absent |
| Use cyber defence tools for continual monitoring and analysis of system activity to identify malicious activity. | Absent |
| Analyse identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. | Absent |
| Determine tactics, techniques, and procedures (TTPs) for intrusion sets. | Absent |
| Examine network topologies to understand data flows through the network. | Absent |
| Recommend computing environment vulnerability corrections. | Absent |
| Identify and Analyse anomalies in network traffic using metadata. | Absent |
| Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). | Absent |
| Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. | Absent |
| Isolate and remove malware. | Absent |
| Identify applications and operating systems of a network device based on network traffic. | Absent |
| Reconstruct a malicious attack or activity based off network traffic. | Absent |
| Identify network mapping and operating system (OS) fingerprinting activities. | Absent |
| Assist in the construction of signatures which can be implemented on cyber defence network tools in response to new or observed threats within the network environment or enclave. | Absent |
| Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan. | Absent |
| Analyse and report organizational security posture trends. | Absent |
| Analyse and report system security posture trends. | Absent |
| Assess adequate access controls based on principles of least privilege and need-to-know. | Absent |
| Monitor external data sources (e.g., cyber defence vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defence threat condition and determine which security issues may have an impact on the enterprise. | Absent |
| Assess and monitor cybersecurity related to system implementation and testing practices. | Absent |
| Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. | Absent |
| Work with stakeholders to resolve computer security incidents and vulnerability compliance. | Absent |
| Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. | Absent |
| Cyber Defence Infrastructure Support Specialist | Coordinate with Cyber Defence Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defence applications. | Absent |
| Perform system administration on specialized cyber defence applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. | Absent |
| Assist in identifying, prioritizing, and coordinating the protection of critical cyber defence infrastructure and key resources. | Absent |
| Build, install, configure, and test dedicated cyber defence hardware. | Absent |
| Assist in assessing the impact of implementing and sustaining a dedicated cyber defence infrastructure. | Absent |
| Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s). | Absent |
| Create, edit, and manage network access control lists on specialized cyber defence systems (e.g., firewalls and intrusion prevention systems). | Absent |
| Identify potential conflicts with implementation of any cyber defence tools (e.g., tool and signature testing and optimization). | Absent |
| Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defence systems within the enterprise, and document and maintain records for them. | Absent |
| Cyber Defence Incident Responder | Coordinate and provide expert technical support to enterprise-wide cyber defence technicians to resolve cyber defence incidents. | Present |
| Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. | Present |
| Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security. | Present |
| Perform cyber defence incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. | Present |
| Perform cyber defence trend analysis and reporting. | Present |
| Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. | Present |
| Perform real-time cyber defence 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 |
| Receive and Analyse network alerts from various sources within the enterprise and determine possible causes of such alerts. | Present |
| Track and document cyber defence incidents from initial detection through final resolution. | Present |
| Write and publish cyber defence techniques, guidance, and reports on incident findings to appropriate constituencies. | Present |
| Employ approved defence-in-depth principles and practices (e.g., defence-in-multiple places, layered defences, security robustness). | Present |
| Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defence incidents within the enterprise. | Present |
| Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. | Present |
| Coordinate with intelligence analysts to correlate threat assessment data. | Present |
| Write and publish after action reviews. | Absent |
| Monitor external data sources (e.g., cyber defence vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defence threat condition and determine which security issues may have an impact on the enterprise. | Absent |
| Coordinate incident response functions. | Present |
| Vulnerability Assessment Analyst | Analyse organization's cyber defence policies and configurations and evaluate compliance with regulations and organizational directives. | Absent |
| Conduct and/or support authorized penetration testing on enterprise network assets. | Absent |
| Maintain deployable cyber defence audit toolkit (e.g., specialized cyber defence software and hardware) to support cyber defence audit missions. | Present |
| Maintain knowledge of applicable cyber defence policies, regulations, and compliance documents specifically related to cyber defence auditing. | Present |
| Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. | Present |
| Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews). | Present |
| Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). | Present |
| Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). | Present |
| Threat/Warning Analyst | Answer requests for information. | Absent |
| Provide subject matter expertise to the development of a common operational picture. | Absent |
| Maintain a common intelligence picture. | Absent |
| Provide subject matter expertise to the development of cyber operations specific indicators. | Absent |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Absent |
| Assist in the identification of intelligence collection shortfalls. | Absent |
| Brief threat and/or target current situations. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Conduct in-depth research and analysis. | Absent |
| Conduct nodal analysis. | Absent |
| Develop information requirements necessary for answering priority information requests. | Absent |
| Evaluate threat decision-making processes. | Absent |
| Identify threats to Blue Force vulnerabilities. | Absent |
| Generate requests for information. | Absent |
| Identify threat tactics, and methodologies. | Absent |
| Identify intelligence gaps and shortfalls. | Absent |
| Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. | Absent |
| Monitor and report on validated threat activities. | Absent |
| Monitor open source websites for hostile content directed towards organizational or partner interests. | Absent |
| Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements. | Absent |
| Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| Provide current intelligence support to critical internal/external stakeholders as appropriate. | Absent |
| Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. | Absent |
| Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. | Absent |
| Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations. | Absent |
| Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. | Absent |
| Report intelligence-derived significant network events and intrusions. | Absent |
| Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date. | Absent |
| Exploitation Analyst | Conduct and/or support authorized penetration testing on enterprise network assets. | Absent |
| Perform penetration testing as required for new or updated applications. | Absent |
| Apply and utilize authorized cyber capabilities to enable access to targeted networks. | Absent |
| Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements. | Absent |
| Apply and obey applicable statutes, laws, regulations and policies. | Absent |
| Perform analysis for target infrastructure exploitation activities. | Absent |
| Collaborate with other internal and external partner organizations on target access and operational issues. | Absent |
| Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers. | Absent |
| Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access. | Absent |
| Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access. | Absent |
| Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities. | Absent |
| Examine intercept-related metadata and content with an understanding of targeting significance. | Absent |
| Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development. | Absent |
| Identify gaps in our understanding of target technology and developing innovative collection approaches. | Absent |
| Identify, locate, and track targets via geospatial analysis techniques. | Absent |
| Lead or enable exploitation operations in support of organization objectives and target requirements. | Absent |
| Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications. | Absent |
| Monitor target networks to provide indications and warning of target communications changes or processing failures. | Absent |
| Produce network reconstructions. | Absent |
| Profile network or system administrators and their activities. | Absent |
| All-Source Analyst | Answer requests for information. | Absent |
| Provide expertise to course of action development. | Absent |
| Provide subject matter expertise to the development of a common operational picture. | Absent |
| Maintain a common intelligence picture. | Absent |
| Provide subject matter expertise to the development of cyber operations specific indicators. | Absent |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Absent |
| Assist in the identification of intelligence collection shortfalls. | Absent |
| Brief threat and/or target current situations. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Conduct in-depth research and analysis. | Absent |
| Conduct nodal analysis. | Absent |
| Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology. | Absent |
| Develop information requirements necessary for answering priority information requests. | Absent |
| Engage customers to understand customers’ intelligence needs and wants. | Absent |
| Evaluate threat decision-making processes. | Absent |
| Identify threat vulnerabilities. | Absent |
| Identify threats to Blue Force vulnerabilities. | Absent |
| Generate requests for information. | Absent |
| Identify threat tactics, and methodologies. | Absent |
| Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. | Absent |
| Identify and submit intelligence requirements for the purposes of designating priority information requirements. | Absent |
| Identify intelligence gaps and shortfalls. | Absent |
| Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. | Absent |
| Monitor and report on validated threat activities. | Absent |
| Monitor open source websites for hostile content directed towards organizational or partner interests. | Absent |
| Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements. | Absent |
| Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| Provide subject matter expertise to website characterizations. | Absent |
| Provide analyses and support for effectiveness assessment. | Absent |
| Provide current intelligence support to critical internal/external stakeholders as appropriate. | Absent |
| Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. | Absent |
| Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. | Absent |
| Provide input and assist in post-action effectiveness assessments. | Absent |
| Provide input and assist in the development of plans and guidance. | Absent |
| Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations. | Absent |
| Provide target recommendations which meet leadership objectives. | Absent |
| Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. | Absent |
| Report intelligence-derived significant network events and intrusions. | Absent |
| Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date. | Absent |
| Mission Assessment Specialist | Provide expertise to course of action development. | Absent |
| Provide subject matter expertise to the development of a common operational picture. | Absent |
| Provide subject matter expertise to the development of cyber operations specific indicators. | Absent |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Absent |
| Provide expertise to the development of measures of effectiveness and measures of performance. | Absent |
| Assist in the identification of intelligence collection shortfalls. | Absent |
| Brief threat and/or target current situations. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Conduct end-of-operations assessments. | Absent |
| Conduct in-depth research and analysis. | Absent |
| Conduct nodal analysis. | Absent |
| Conduct target research and analysis. | Absent |
| Develop information requirements necessary for answering priority information requests. | Absent |
| Develop measures of effectiveness and measures of performance. | Absent |
| Develop munitions effectiveness assessment or operational assessment materials. | Absent |
| Engage customers to understand customers’ intelligence needs and wants. | Absent |
| Estimate operational effects generated through cyber activities. | Absent |
| Evaluate threat decision-making processes. | Absent |
| Identify threat vulnerabilities. | Absent |
| Generate requests for information. | Absent |
| Identify intelligence gaps and shortfalls. | Absent |
| Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. | Absent |
| Monitor and report on validated threat activities. | Absent |
| Monitor operational environment and report on adversarial activities which fulfil leadership’s priority information requirements. | Absent |
| Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| Provide analyses and support for effectiveness assessment. | Absent |
| Provide current intelligence support to critical internal/external stakeholders as appropriate. | Absent |
| Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. | Absent |
| Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. | Absent |
| Provide input and assist in post-action effectiveness assessments. | Absent |
| Provide input and assist in the development of plans and guidance. | Absent |
| Provide effectiveness support to designated exercises, and/or time sensitive operations. | Absent |
| Provide target recommendations which meet leadership objectives. | Absent |
| Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date. | Absent |
| Target Developer | Accurately characterize targets. | Absent |
| Provide expertise to course of action development. | Absent |
| Provide expertise to the development of measures of effectiveness and measures of performance. | Absent |
| Build and maintain electronic target folders. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas. | Absent |
| Conduct nodal analysis. | Absent |
| Conduct target research and analysis. | Absent |
| Coordinate target vetting with appropriate partners. | Absent |
| Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology. | Absent |
| Determine what technologies are used by a given target. | Absent |
| Develop all-source intelligence targeting materials. | Absent |
| Develop measures of effectiveness and measures of performance. | Absent |
| Develop munitions effectiveness assessment or operational assessment materials. | Absent |
| Estimate operational effects generated through cyber activities. | Absent |
| Evaluate available capabilities against desired effects to recommend efficient solutions. | Absent |
| Generate requests for information. | Absent |
| Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. | Absent |
| Identify critical target elements. | Absent |
| Initiate requests to guide tasking and assist with collection management. | Absent |
| Maintain target lists (i.e., RTL, JTL, CTL, etc.). | Absent |
| Perform targeting automation activities. | Absent |
| Characterize websites. | Absent |
| Produce target system analysis products. | Absent |
| Provide aim point and reengagement recommendations. | Absent |
| Provide analyses and support for effectiveness assessment. | Absent |
| Provide input for targeting effectiveness assessments for leadership acceptance. | Absent |
| Provide operations and reengagement recommendations. | Absent |
| Provide target recommendations which meet leadership objectives. | Absent |
| Provide targeting products and targeting support as designated. | Absent |
| Provide time sensitive targeting support. | Absent |
| Review appropriate information sources to determine validity and relevance of information gathered. | Absent |
| Sanitize and minimize information to protect sources and methods. | Absent |
| Support identification and documentation of collateral effects. | Absent |
| Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date. | Absent |
| Target Network Analyst | Provide expertise to course of action development. | Absent |
| Classify documents in accordance with classification guidelines. | Absent |
| Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas. | Absent |
| Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. | Absent |
| Identify and conduct analysis of target communications to identify information essential to support operations. | Absent |
| Conduct nodal analysis. | Absent |
| Conduct quality control to determine validity and relevance of information gathered about networks. | Absent |
| Conduct target research and analysis. | Absent |
| Determine what technologies are used by a given target. | Absent |
| Apply analytic techniques to gain more target information. | Absent |
| Generate and evaluate the effectiveness of network analysis strategies. | Absent |
| Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.) | Absent |
| Generate requests for information. | Absent |
| Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. | Absent |
| Identify collection gaps and potential collection strategies against targets. | Absent |
| Identify network components and their functionality to enable analysis and target development. | Absent |
| Make recommendations to guide collection in support of customer requirements. | Absent |
| Provide subject matter expertise to development of exercises. | Absent |
| Perform content and/or metadata analysis to meet organization objectives. | Absent |
| Profile targets and their activities. | Absent |
| Provide target recommendations which meet leadership objectives. | Absent |
| Review appropriate information sources to determine validity and relevance of information gathered. | Absent |
| Reconstruct networks in diagram or report format. | Absent |
| Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources. | Absent |
| Multi-Disciplined Language Analyst | Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. | Absent |
| Determine what technologies are used by a given target. | Absent |
| Identify collection gaps and potential collection strategies against targets. | Absent |
| Make recommendations to guide collection in support of customer requirements. | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| Advise managers and operators on language and cultural issues that impact organization objectives. | Absent |
| Analyse and process information using language and/or cultural expertise. | Absent |
| Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities. | Absent |
| Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination. | Absent |
| Conduct all-source target research to include the use of open-source materials in the target language. | Absent |
| Conduct analysis of target communications to identify essential information in support of organization objectives. | Absent |
| Perform quality review and provide feedback on transcribed or translated materials. | Absent |
| Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing. | Absent |
| Identify cyber threat tactics and methodologies. | Absent |
| Identify target communications within the global network. | Absent |
| Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis. | Absent |
| Provide feedback to collection managers to enhance future collection and analysis. | Absent |
| Perform foreign language and dialect identification in initial source data. | Absent |
| Perform or support technical network analysis and mapping. | Absent |
| Provide requirements and feedback to optimize the development of language processing tools. | Absent |
| Perform social network analysis and document as appropriate. | Absent |
| Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material. | Absent |
| Tip critical or time-sensitive information to appropriate customers. | Absent |
| Transcribe target voice materials in the target language. | Absent |
| Translate (e.g., verbatim, gist, and/or summaries) target graphic material. | Absent |
| Translate (e.g., verbatim, gist, and/or summaries) target voice material. | Absent |
| Identify foreign language terminology within computer programs (e.g., comments, variable names). | Absent |
| Provide near-real time language analysis support (e.g., live operations). | Absent |
| Identify cyber/technology-related terminology in the target language. | Absent |
| All Source-Collection Manager | Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements. | Absent |
| Analyse feedback to determine extent to which collection products and services are meeting requirements. | Absent |
| Analyse 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 |
| Assess and apply operational environment factors and risks to collection management process. | Absent |
| Assess performance of collection assets against prescribed specifications. | Absent |
| Compare allocated and available assets to collection demand as expressed through requirements. | Absent |
| Compile lessons learned from collection management activity's execution of organization collection objectives. | Absent |
| Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements. | Absent |
| Construct collection plans and matrixes using established guidance and procedures. | Absent |
| Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads. | Absent |
| Coordinate inclusion of collection plan in appropriate documentation. | Absent |
| Re-task or re-direct collection assets and resources. | Absent |
| Determine course of action for addressing changes to objectives, guidance, and operational environment. | Absent |
| Determine existing collection management webpage databases, libraries and storehouses. | Absent |
| Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function. | Absent |
| Determine organizations and/or echelons with collection authority over all accessible collection assets. | Absent |
| Develop a method for comparing collection reports to outstanding requirements to identify information gaps. | Absent |
| Develop coordinating instructions by collection discipline for each phase of an operation. | Absent |
| Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis. | Absent |
| Disseminate tasking messages and collection plans. | Absent |
| Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems. | Absent |
| Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures. | Absent |
| Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers. | Absent |
| Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables. | Absent |
| Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups. | Absent |
| Identify coordination requirements and procedures with designated collection authorities. | Absent |
| Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness. | Absent |
| Identify potential collection disciplines for application against priority information requirements. | Absent |
| Identify and mitigate risks to collection management ability to support the plan, operations and target cycle. | Absent |
| Issue requests for information. | Absent |
| Link priority collection requirements to optimal assets and resources. | Absent |
| Monitor completion of reallocated collection efforts. | Absent |
| Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture. | Absent |
| Monitor the operational environment for potential factors and risks to the collection operation management process. | Absent |
| Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements. | Absent |
| Prioritize collection requirements for collection platforms based on platform capabilities. | Absent |
| Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations. | Absent |
| Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures. | Absent |
| Review capabilities of allocated collection assets. | Absent |
| Review intelligence collection guidance for accuracy/applicability. | Absent |
| Review list of prioritized collection requirements and essential information. | Absent |
| Review and update overarching collection plan, as required. | Absent |
| Revise collection matrix based on availability of optimal assets and resources. | Absent |
| Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources. | Absent |
| Specify discipline-specific collections and/or taskings that must be executed in the near term. | Absent |
| Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques. | Absent |
| All Source-Collection Requirements Manager | Analyse feedback to determine extent to which collection products and services are meeting requirements. | Absent |
| Analyse incoming collection requests. | Absent |
| Analyse 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 |
| Assess efficiency of existing information exchange and management systems. | Absent |
| Assess performance of collection assets against prescribed specifications. | Absent |
| Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and adjust collection strategies and collection requirements accordingly. | Absent |
| Close requests for information once satisfied. | Absent |
| Collaborate with customer to define information requirements. | Absent |
| Compile lessons learned from collection management activity's execution of organization collection objectives. | Absent |
| Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures. | Absent |
| Develop a method for comparing collection reports to outstanding requirements to identify information gaps. | Absent |
| Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centres. | Absent |
| Disseminate reports to inform decision makers on collection issues. | Absent |
| Conduct and document an assessment of the collection results using established procedures. | Absent |
| Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership. | Absent |
| Evaluate extent to which collected information and/or produced intelligence satisfy information requests. | Absent |
| Evaluate extent to which collection operations are synchronized with operational requirements. | Absent |
| Evaluate the effectiveness of collection operations against the collection plan. | Absent |
| Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups. | Absent |
| Identify and mitigate risks to collection management ability to support the plan, operations and target cycle. | Absent |
| Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures. | Absent |
| Issue requests for information. | Absent |
| Modify collection requirements as necessary. | Absent |
| Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans. | Absent |
| Review capabilities of allocated collection assets. | Absent |
| Review intelligence collection guidance for accuracy/applicability. | Absent |
| Review list of prioritized collection requirements and essential information. | Absent |
| Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements. | Absent |
| Submit information requests to collection requirement management section for processing as collection requests. | Absent |
| Track status of information requests, including those processed as collection requests and production requirements, using established procedures. | Absent |
| Translate collection requests into applicable discipline-specific collection requirements. | Absent |
| Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness. | Absent |
| Validate requests for information according to established criteria. | Absent |
| Cyber Intel Planner | Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives. | Absent |
| Coordinate for intelligence support to operational planning activities. | Absent |
| Assess all-source intelligence and recommend targets to support cyber operation objectives. | Absent |
| Assess target vulnerabilities and/or operational capabilities to determine course of action. | Absent |
| Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. | Absent |
| Assist in the development and refinement of priority information requirements. | Absent |
| Enable synchronization of intelligence support plans across partner organizations as required. | Absent |
| Provide input to the identification of cyber-related success criteria. | Absent |
| Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials). | Absent |
| Contribute to crisis action planning for cyber operations. | Absent |
| Contribute to the development of the organization's decision support tools if necessary. | Absent |
| Incorporate intelligence equities into the overall design of cyber operations plans. | Absent |
| Coordinate with intelligence planners to ensure that collection managers receive information requirements. | Absent |
| Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks. | Absent |
| Coordinate, produce, and track intelligence requirements. | Absent |
| Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans. | Absent |
| Use intelligence estimates to counter potential target actions. | Absent |
| Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives. | Absent |
| Develop and review intelligence guidance for integration into supporting cyber operations planning and execution. | Absent |
| Develop detailed intelligence support to cyber operations requirements. | Absent |
| Develop potential courses of action. | Absent |
| Develop, implement, and recommend changes to appropriate planning procedures and policies. | Absent |
| Draft cyber intelligence collection and production requirements. | Absent |
| Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines. | Absent |
| Evaluate intelligence estimates to support the planning cycle. | Absent |
| Evaluate the conditions that affect employment of available cyber intelligence capabilities. | Absent |
| Incorporate intelligence and counterintelligence to support plan development. | Absent |
| Identify all available partner intelligence capabilities and limitations supporting cyber operations. | Absent |
| Identify, draft, evaluate, and prioritize relevant intelligence or information requirements. | Absent |
| Identify cyber intelligence gaps and shortfalls for cyber operational planning. | Absent |
| Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production. | Absent |
| Provide input to or develop courses of action based on threat factors. | Absent |
| Interpret environment preparations assessments to determine a course of action. | Absent |
| Issue requests for information. | Absent |
| Lead and coordinate intelligence support to operational planning. | Absent |
| Maintain relationships with internal and external partners involved in cyber planning or related areas. | Absent |
| Maintain situational awareness to determine if changes to the operating environment require review of the plan. | Absent |
| Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary. | Absent |
| Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| Prepare for and provide subject matter expertise to exercises. | Absent |
| Provide cyber focused guidance and advice on intelligence support plan inputs. | Absent |
| Recommend refinement, adaption, termination, and execution of operational plans as appropriate. | Absent |
| Review and comprehend organizational leadership objectives and guidance for planning. | Absent |
| Scope the cyber intelligence planning effort. | Absent |
| Document lessons learned that convey the results of events and/or exercises. | Absent |
| Cyber Ops Planner | Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines. | Absent |
| Evaluate intelligence estimates to support the planning cycle. | Absent |
| Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives. | Absent |
| Gather and Analyse data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities. | Absent |
| Incorporate cyber operations and communications security support plans into organization objectives. | Absent |
| Identify cyber intelligence gaps and shortfalls for cyber operational planning. | Absent |
| Integrate cyber planning/targeting efforts with other organizations. | Absent |
| Interpret environment preparations assessments to determine a course of action. | Absent |
| Issue requests for information. | Absent |
| Maintain relationships with internal and external partners involved in cyber planning or related areas. | Absent |
| Maintain situational awareness of cyber-related intelligence requirements and associated tasking. | Absent |
| Maintain situational awareness of partner capabilities and activities. | Absent |
| Maintain situational awareness to determine if changes to the operating environment require review of the plan. | Absent |
| Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives. | Absent |
| Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| Provide subject matter expertise to planning efforts with internal and external cyber operations partners. | Absent |
| Prepare for and provide subject matter expertise to exercises. | Absent |
| Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs. | Absent |
| Provide input to the administrative and logistical elements of an operational support plan. | Absent |
| Provide planning support between internal and external partners. | Absent |
| Recommend refinement, adaption, termination, and execution of operational plans as appropriate. | Absent |
| Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities. | Absent |
| Submit or respond to requests for deconfliction of cyber operations. | Absent |
| Document lessons learned that convey the results of events and/or exercises. | Absent |
| Partner Integration Planner | Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement. | Absent |
| Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. | Absent |
| Provide expertise to course of action development. | Absent |
| Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials). | Absent |
| Contribute to crisis action planning for cyber operations. | Absent |
| Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers. | Absent |
| Coordinate with intelligence and cyber defence partners to obtain relevant essential information. | Absent |
| Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations. | Absent |
| Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives. | Absent |
| Develop strategy and processes for partner planning, operations, and capability development. | Absent |
| Develop, implement, and recommend changes to appropriate planning procedures and policies. | Absent |
| Develop, maintain, and assess cyber cooperation security agreements with external partners. | Absent |
| Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives. | Absent |
| Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community. | Absent |
| Identify and manage security cooperation priorities with external partners. | Absent |
| Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities. | Absent |
| Integrate cyber planning/targeting efforts with other organizations. | Absent |
| Maintain relationships with internal and external partners involved in cyber planning or related areas. | Absent |
| Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives. | Absent |
| Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy. | Absent |
| Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary. | Absent |
| Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| Provide subject matter expertise to planning efforts with internal and external cyber operations partners. | Absent |
| Propose policy which governs interactions with external coordination groups. | Absent |
| Prepare for and provide subject matter expertise to exercises. | Absent |
| Provide cyber focused guidance and advice on intelligence support plan inputs. | Absent |
| Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs. | Absent |
| Provide planning support between internal and external partners. | Absent |
| Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations. | Absent |
| Serve as a liaison with external partners. | Absent |
| Submit or respond to requests for deconfliction of cyber operations. | Absent |
| Synchronize cyber international engagement activities and associated resource requirements as appropriate. | Absent |
| Synchronize cyber portions of security cooperation plans. | Absent |
| Document lessons learned that convey the results of events and/or exercises. | Absent |
| Cyber Operator | Analyse internal operational architecture, tools, and procedures for ways to improve performance. | Absent |
| Analyse target operational architecture for ways to gain access. | Absent |
| Collaborate with development organizations to create and deploy the tools needed to achieve objectives. | Absent |
| Conduct access enabling of wireless computer and digital networks. | Absent |
| Conduct collection and processing of wireless computer and digital networks. | Absent |
| Conduct exploitation of wireless computer and digital networks. | Absent |
| Conduct network scouting and vulnerability analyses of systems within a network. | Absent |
| Conduct on-net activities to control and exfiltrate data from deployed technologies. | Absent |
| Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies. | Absent |
| Conduct open source data collection via various online tools. | Absent |
| Conduct survey of computer and digital networks. | Absent |
| Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers). | Absent |
| Detect exploits against targeted networks and hosts and react accordingly. | Absent |
| Develop new techniques for gaining and keeping access to target systems. | Absent |
| Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems. | Absent |
| Exploit network devices, security devices, and/or terminals or environments using various methods or tools. | Absent |
| Facilitate access enabling by physical and/or wireless means. | Absent |
| Identify potential points of strength and vulnerability within a network. | Absent |
| Maintain situational awareness and functionality of organic operational infrastructure. | Absent |
| Operate and maintain automated systems for gaining and maintaining access to target systems. | Absent |
| Conduct cyber activities to degrade/remove information resident in computers and computer networks. | Absent |
| Process exfiltrated data for analysis and/or dissemination to customers. | Absent |
| Provide real-time actionable geolocation information. | Absent |
| Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects. | Absent |
| Test and evaluate locally developed tools for operational use. | Absent |
| Test internal developed tools and techniques against target tools. | Absent |
| Cyber Crime Investigator | Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects. | Absent |
| Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. | Absent |
| Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals). | Absent |
| Examine recovered data for information of relevance to the issue at hand. | Absent |
| Fuse computer network attack analyses with criminal and counterintelligence investigations and operations. | Absent |
| Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action. | Absent |
| Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations. | Absent |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. | Absent |
| Identify elements of proof of the crime. | Absent |
| Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations. | Absent |
| Process crime scenes. | Absent |
| Secure the electronic device or information source. | Absent |
| Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. | Absent |
| Analyse the crisis to ensure public, personal, and resource protection. | Absent |
| Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation. | Absent |
| Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks. | Absent |
| Provide criminal investigative support to trial counsel during the judicial process. | Absent |
| Analyse computer-generated threats for counter intelligence or criminal activity. | Absent |
| Gather and preserve evidence used on the prosecution of computer crimes. | Absent |
| Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes. | Absent |
| Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes. | Absent |
| Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking). | Absent |
| Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property. | Absent |
| Prepare reports to document the investigation following legal standards and requirements. | Absent |
| Law Enforcement /Counterintelligence Forensics Analyst | Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. | Absent |
| Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals). | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Analyse incident data for emerging trends. | Absent |
| Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. | Absent |
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. | Absent |
| Maintain deployable cyber defence toolkit (e.g., specialized cyber defence software/hardware) to support Incident Response Team mission. | Absent |
| Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data). | Absent |
| Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. | Absent |
| Analyse organizational cyber policy. | Absent |
| Cyber Defence Forensics Analyst | Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. | Absent |
| Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. | Absent |
| Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats. | Absent |
| Decrypt seized data using technical means. | Absent |
| Provide technical summary of findings in accordance with established reporting procedures. | Absent |
| Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence. | Absent |
| Examine recovered data for information of relevance to the issue at hand. | Absent |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. | Absent |
| Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment. | Absent |
| Perform file signature analysis. | Absent |
| Perform hash comparison against established database. | Absent |
| Perform real-time forensic analysis (e.g., using Helix in conjunction with Live View). | Absent |
| Perform timeline analysis. | Absent |
| Perform real-time cyber defence incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). | Absent |
| Perform static media analysis. | Absent |
| Perform tier 1, 2, and 3 malware analysis. | Absent |
| Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures). | Absent |
| Provide technical assistance on digital evidence matters to appropriate personnel. | Absent |
| Recognize and accurately report forensic artifacts indicative of a particular operating system. | Absent |
| Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost). | Absent |
| Capture and Analyse network traffic associated with malicious activities using network monitoring tools. | Absent |
| Use specialized equipment and techniques to catalogue, document, extract, collect, package, and preserve digital evidence. | Absent |
| Conduct cursory binary analysis. | Absent |
| Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. | Absent |
| Perform virus scanning on digital media. | Absent |
| Perform file system forensic analysis. | Absent |
| Perform static analysis to mount an "image" of a drive (without necessarily having the original drive). | Absent |
| Perform static malware analysis. | Absent |
| Utilize deployable forensics toolkit to support operations as necessary. | Absent |
| Coordinate with intelligence analysts to correlate threat assessment data. | Absent |
| Process image with appropriate tools depending on analyst’s goals. | Absent |
| Perform Windows registry analysis. | Absent |
| Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. | Absent |
| Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired. | Absent |
| Correlate incident data and perform cyber defence reporting. | Absent |
| Maintain deployable cyber defence toolkit (e.g., specialized cyber defence software/hardware) to support Incident Response Team mission. | Absent |
| Collect and Analyse intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defence incidents within the enterprise. | Absent |
| Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information. | Absent |
| Write and publish cyber defence recommendations, reports, and white papers on incident findings to appropriate constituencies. | Absent |

**List of potential threats to Boston Orthopedics that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, cybersecurity work roles and Cybersecurity Tasks**

|  |
| --- |
| **Threats** |
| Potential compromise of the Database, Unable to access any machine within the organization. |
| Loss of Confidentiality, Data Privacy, and Availability. Nonrepudiation. |
| Potential compromise of the Database, Unable to access any machine within the organization. |
| Information Theft, Unauthorized access, unprotected wireless network |
| Disruption of Business lifecycles |
| Non-Compliance with Data Privacy |
| Loss of Confidentiality, Trustworthiness, goodwill, and Privacy |
| Disruption of Business lifecycles |
| Critical Data Theft |
| Potential sensitive information disclosure |

**List of potential risks to Boston Orthopedics that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, cybersecurity work roles and Cybersecurity Tasks**

|  |
| --- |
| **Risks** |
| Provide access to critically sensitive data to Bad vectors. The smart card acts as a physical access token and is unique. |
| Can make systems/servers compromise easily if ports were not blocked and monitored. |
| Information theft is made easy if the DoD common access card is not present. |
| Password controls have to be followed to not Provide access to critically sensitive data to Bad vectors |
| The latest technologies are harder to crack, older techniques might leverage bad vectors. |
| Provide access to critically sensitive data to Bad vectors. Wireless sessions need to be secured against man-in-the-middle attacks. |
| Information Theft, Unauthorized access, Weak access, Sensitive data exposure |
| Weak network infrastructure, Information Theft, Unauthorized access |
| Provide access to critically sensitive data to Bad vectors. Router planes must be secured in order to minimize attacks on routers. |
| Information theft is made easy if the DoD controls not present. |

**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**

* Before developing a compliance program, auditing companies must first examine the total risk in broad and adsorptive properties.
* Confidentiality, Integrity, Availability, Effectiveness, Compliance, Authenticity, Operation, and Capability are all considered while evaluating computer networks.
* To collect substantial proof, auditors should develop and select an auditing sample, conduct audit processes, and analyze the outcomes.
* Check whether procedures and processes put in place, evaluate whether team understands the established policies and procedures, and confirm that the policy and practices are being compliant while reviewing that's Is policies and processes.
* Generates a feeling of controlling ownership among system administrators.
* To fulfill the organization's overall objectives, business and IT processes should be coordinated.
* It is critical that Board of Directors and the CEO work together.
* Determine the most important systems and processes as well as the technological infrastructures.
* Regulations must assist the attainment of corporate goals as well as the deployment of information security controls.
* Top leadership should establish the information security program, which should then be written and articulated to all relevant persons, including customers, network operators, and business associates.
* The existing risk management policy should be communicated to all employees.
* It should be evaluated on a regular basis, at least once a year.
* The owner of the information security program should have approved the responsibility for the management for the policy's creation, implementation, and assessment.
* Prioritize the incident's management based on the assessment and follow the protocol to declare a catastrophe if necessary.
* Before transferring personal information to another country, organizations should get sufficient consent.
* Personal information should be acquired for certain purposes, which should be specified by organizations.
* Companies must have a good governance system in place for third-party services.
* For users to acquire access to the information under their control, the system administrator should offer written authorization or stated rules.
* The organization must make sure that contract has enough indemnity measures to safeguard them from potential damages caused either by third party's activities.

**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**

I believe that HGA has addressed most of the critical security risks and the new controls proposed by the new CISO and team are covering most of them. However, I feel like there are many other controls that could be considered.

Only the Incident Response team is considered in HGA, but there must be other teams such as Red Team which works on the offensive side to identify more vulnerabilities thus providing more chance of assessing the accurate risk when seen from an attacker’s perspective.

The addition of many new tools and software and processes must be taken into consideration to protect endpoints, new software and mitigate the third part risks as well. I believe still there is room to grow for HGA and the new CISO team to concentrate in these areas. Phishing is a great threat to any organization and perfect controls to defend against phishing attacks are lacking in the proposed controls.

As per the assessments, the addition of VPN and DMZ to the HGA network architecture is seen as a proactive step by the HGA executive board. However, the installation of VPN introduces new vulnerabilities and threats, increasing the risk. Controls linked to VPN were not handled in HGA's new and old controls. Because VPN poses a significant risk because employees can connect to the company's internal network from anywhere, extra traffic monitoring and firewall implementation must be considered. Meanwhile, the DMZ is used to minimize risks from outside the internal network, and every DMZ hit must be examined for any potentially suspicious activity and IOC's blocked.

To make the environment safer, the DMZ zone might be used more effectively to reduce external threats, and regular scanning of the DMZ zone is required. Many of the MOT controls that were installed failed to address important security issues like email security, antivirus, and endpoint firewalls. MOT controls are primarily focused on payroll operations and risks, but a broader view of network topology is also required. Because it has a WAN link in addition to the internet, an attacker might use lateral movement to obtain access to HGA if other agencies were hacked. As a result, IAM, Emergency Lockdown, and the isolation of affected machines must all be implemented. The firewall is also important for preventing lateral movement. Policies in the network such as local perimeter and edge perimeter, as well as DMZ, are regarded as a good solution since they improve the overall security posture, and new or old MOT controls have failed to meet the dangers posed by the above.

I would strongly advise using a mixed strategy approach, as evidenced by the above-mentioned document, which states that the mixed strategy is the most effective method for reducing risk to a medium level.

The outcomes are more gratifying when both risk prevention and risk response strategies are combined and handled, as the residual risk connected with the view of assets and vulnerabilities is considered.

A blended strategy, on the other hand, could not be directly approached. It is necessary to execute a risk prevention plan first, followed by a risk response strategy. As a result, work on the two types of strategies must be addressed separately in the context of real-time risk assessment execution. Because risks must be handled on a regular basis, a mixed strategy cannot be applied directly.

**Provide the total cost and benefit in $ for the recommended controls, methods and policies**

**based on your security risk management analysis**

**For HGA:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Controls mitigating** | **Risk Prevention Budget** | **Risk Response Budget** | **Mixed Strategy Budget** |
| Payroll Frauds | $60,000 | $40,000 | $90,000 |
| Unauthorized Access | $70,000 | $110,000 | $170,000 |
| Network Threats | $45,000 | $55,000 | $90,000 |
| Email Threats | $80,000 | $40,000 | $110,000 |
| Data Loss Prevention techniques | $90,000 | $60,000 | $140,000 |
| Data Classification and Backups | $60,000 | $80,000 | $130,000 |
| Dedicated Incident Response Team | $130,000 | $90,000 | $210,000 |
| Security Trainings for Employees | $60,000 | $70,000 | $120,000 |
| DMZ | $30,000 | $40,000 | $60,000 |
| VPN | $20,000 | $30,000 | $40,000 |
| Physical Security of Assets | $60,000 | $120,000 | $170,000 |
| **Total** | **$705,000** | **$735,000** | **$1,330,000** |

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

**$2,705,000 - $411,592 = $2,293,408**

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

**Proposed Security Budget cost for 3 Budgets:**

* Cost-benefit ratio analysis for Risk Prevention Budget
* Proposed Security Risk Budget Cost / Expected Security Risk-Benefit
* **705000 / 2293408 = 0.307**
* Cost-benefit ratio analysis for Risk Resilience Budget
* Proposed Security Risk Budget Cost / Expected Security Risk-Benefit
* **735000 / 2293408 = 0.320**
* Cost-benefit ratio analysis for Mixed Budget
* Proposed Security Risk Budget Cost / Expected Security Risk-Benefit
* **1330000 / 2293408 = 0.579**

**For Boston Orthopedics:**

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

**$51 Million - $23 Million = $28 Million**

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

**Proposed Security Budget cost for 3 Budgets:**

* Cost-benefit ratio analysis for Mixed Budget
* Proposed Security Risk Budget Cost / Expected Security Risk-Benefit
* **21 Million / $28 Million = 0.75**

**Comparing the proposed security controls, methods, and polices budget for HGA with the proposed security controls, methods, and policies budget for Boston Orthopedics**

|  |  |  |
| --- | --- | --- |
| **Points of Consideration** | **HGA** | **Boston Orthopedics** |
| Industry | Government - Financial | Medical |
| Mission | Deals with payments across various government agencies and employees | Design and Manufacture Medical Devices |
| Geographic Presence | United States of America | Across the Globe |
| Number of Employees | 1000 | 40000 |
| Network Topology | Appendix 3 | Appendix 4 |
| Critical Assets | $27,050,000 | $51 Million |
| Threat Environment | Nation State, Competitors, Hacker Organizations | Nation State, Competitors, Hacker Organizations, Insider Threat |
| Threat Agents | Cyber Terrorists, Cyber Criminals, Insiders | Script kiddies, State sponsored groups |
| Residual Risks in $ | **$2,293,408** | $28 Million |
| Budget for Risk Prevention and Response controls, methods, and policies | $1,330,000 | $21 Million |
| $ Security Budget / $ Security Risk Improvements | **0.32** | 0.56 |
| $ Security Budget / $ Critical Assets | 0.56 | 0.75 |
| $ Security Budget / $ Employees | 530 | 800 |

**Attack Trees for HGA:**

**Diagram

Description automatically generated**

**Attack Trees for Boston Orthopedics:**

**Diagram

Description automatically generated**

**Vulnerabilities and Exploitation Probabilities:**

**For HGA:**

|  |  |
| --- | --- |
| **Vulnerability** | **Exploitation Probability** |
| Time Sheets Manipulation | 67 |
| Manipulation of Payroll System Entries | 43 |
| Fraudulent employee records | 28 |
| Not following Virus Prevention Analysis | 91 |
| Sensitive Information Disclosure | 87 |
| Unauthorized Access to Sensitive Information | 39 |
| Lack of Authentication mechanisms | 23 |
| Unsecured user Accounts | 88 |
| Lack of Information Security Policies | 76 |
| Contingency Planning errors | 54 |
| Vulnerabilities of Network-Related Attacks | 70 |

**For Boston Orthopedics:**

|  |  |
| --- | --- |
| **Vulnerability** | **Exploitation Probability** |
| Critical Data Theft | 39 |
| Potential sensitive information disclosure | 23 |
| Unauthorized Access to Servers/Workstations | 88 |
| Backdoor establishments | 76 |
| Social Engineering | 65 |
| Weak network infrastructure | 67 |
| Potential sensitive information disclosure | 43 |
| Unauthorized Access to Servers/Workstations | 28 |
| Backdoor establishments | 91 |
| Unprotected wireless network | 87 |
| Sensitive data exposure and Information Theft | 34 |

**Cybersecurity Workforce Recommendations:**

**For HGA:**

* The outcomes are more gratifying when both risk prevention and risk response strategies are combined and handled, as the residual risk connected with the view of assets and vulnerabilities is considered.
* A blended strategy, on the other hand, could not be directly approached.
* It is necessary to execute a risk prevention plan first, followed by a risk response strategy. As a result, work on the two types of strategies must be addressed separately in the context of real-time risk assessment execution.
* Because risks must be handled on a regular basis, a mixed strategy cannot be applied directly.
* Regulations must assist the attainment of corporate goals as well as the deployment of information security controls.
* Top leadership should establish the information security program, which should then be written and articulated to all relevant persons, including customers, network operators, and business associates.
* The existing risk management policy should be communicated to all employees

**For Boston Orthopedics:**

* Check whether procedures and processes put in place, evaluate whether team understands the established policies and procedures, and confirm that the policy and practices are being compliant while reviewing that's Is policies and processes.
* Generates a feeling of controlling ownership among system administrators.
* To fulfill the organization's overall objectives, business and IT processes should be coordinated.
* It is critical that Board of Directors and the CEO work together.
* Determine the most important systems and processes as well as the technological infrastructures.
* Regulations must assist the attainment of corporate goals as well as the deployment of information security controls.
* Top leadership should establish the information security program, which should then be written and articulated to all relevant persons, including customers, network operators, and business associates.
* The existing risk management policy should be communicated to all employees.
* It should be evaluated on a regular basis, at least once a year.
* The owner of the information security program should have approved the responsibility for the management for the policy's creation, implementation, and assessment.
* Prioritize the incident's management based on the assessment and follow the protocol to declare a catastrophe if necessary.

**Part D: Appendix**

**Appendix 3:**

**Network Topology of HGA**



The network topology of the HGA can be explained considering the most critical and central part of it, which is WAN (Wide Area Network). WAN is integrating the LAN of HGA to the Other agency LAN networks and to the private database and model pool. Within the HGA LAN, it is connected to an administrative console and modem pool along with the critical infrastructure of HGA such as its systems, servers, and printers. This type of connection is very practical and most effective in terms of security as the internal network is isolated from the external and centralized components manages the network traffic without impacting the critical infrastructure.

**Appendix 4:**

**Network Topology of Boston Orthopedics:**

**Diagram

Description automatically generated**

The above network topology describes the infrastructure and network configuration of Boston orthopedics. The company uses various machines, servers, and throughout the organization. Network security elements like Firewalls are also in place. In the network, a LAN server is present that is responsible for the connectivity within the company. And it is connected to a router where it manages the external traffic routing. The company also uses VPN so that external networks could connect to internal networks using VPN.

**References:**

Security policy templates. Information Security Policy Templates | SANS Institute. (n.d.). Retrieved March 13, 2022, from [https://www.sans.org/information-security-policy/](https://www.sans.org/information-security-policy/?category=network-security)

Online diagram software &amp; visual solution. Lucidchart. (n.d.). Retrieved March 13, 2022, from <https://www.lucidchart.com/>

Wikimedia Foundation. (2022, February 21). Extensible authentication protocol. Wikipedia. Retrieved April 17, 2022, from https://en.wikipedia.org/wiki/Extensible\_Authentication\_Protocol

Global Cybersecurity leader. Palo Alto Networks. (n.d.). Retrieved March 13, 2022, from https://www.paloaltonetworks.com/

HGA Case Study

<https://www.cisa.gov/uscert/bsi/articles/best-practices/architectural-risk-analysis>

Security policy templates. Information Security Policy Templates | SANS Institute. (n.d.). Retrieved March 13, 2022, from <https://www.sans.org/information-security-policy/?category=network-security>

https://www.bitsight.com/blog/cio-vs-ciso (Links to an external site.)

<https://www.commoncriteriaportal.org/ccra/index.cfm>

[https://www.cyberark.com/ (Links to an external site.)](https://www.cyberark.com/ (Links%20to%20an%20external%20site.))

[https://www.okta.com/ (Links to an external site.)](https://www.okta.com/ (Links%20to%20an%20external%20site.))

[https://en.wikipedia.org/wiki/Active\_Directory (Links to an external site.)](https://en.wikipedia.org/wiki/Active_Directory (Links%20to%20an%20external%20site.))

[https://www.microsoft.com/en-us/security/business/identity-access-management/mfa-multi-factor-authentication (Links to an external site.)](https://www.microsoft.com/en-us/security/business/identity-access-management/mfa-multi-factor-authentication (Links%20to%20an%20external%20site.))

[https://www.onetrust.com/ (Links to an external site.)](https://www.onetrust.com/ (Links%20to%20an%20external%20site.))

<https://www.secureone.com/>

<https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.180.4844&rep=rep1&type=pdf>

<https://www.varonis.com/blog/ipv6-security>

Mk, Chugh, A., Horus, Bagal, R., Tako, I., Yetra, A., Rocks, Fatima, Kalayu, K., Mazenet, Gowtham, T., Ram, Routclough, R., Reddy, R., Tomar, M., dazzy, E., Raja, Faith, Kirti, … Adam, A. (2022, March 3). *Penetration testing - complete guide with penetration testing sample test cases*. Software Testing Help. Retrieved March 13, 2022, from <https://www.softwaretestinghelp.com/penetration-testing-guide/>

The advantages and the implementation of SSL VPN. IEEE Xplore. (n.d.). Retrieved March 27, 2022, from https://ieeexplore.ieee.org/document/5982375 (Links to an external site.)

Uum Repository. Welcome to UUM Repository - UUM Repository. (n.d.). Retrieved March 27, 2022, from http://repo.uum.edu.my/ (Links to an external site.)

2007 10 IPv6 report final Revappv3 - Energy.gov. (n.d.). Retrieved March 27, 2022, from <https://www.energy.gov/sites/default/files/oeprod/DocumentsandMedia/22-Impacts_of_IPv6_on_CS.pdf>

Archiveddocs. (n.d.). Managing the New Wireless Network (IEEE 802.11) policies settings. Microsoft Docs. Retrieved April 17, 2022, from https://docs.microsoft.com/en-us/previous-versions/windows/it-pro/windows-server-2012-R2-and-2012/hh994701(v=ws.11) (Links to an external site.)

https://ieeexplore.ieee.org/document/1176303 (Links to an external site.)

https://www.researchgate.net/publication/4055016\_Architectures\_for\_intrusion\_tolerant\_database\_systems