

**CY 5200: Security Risk Management and Assessment Class Paper**

Instructor: Professor Themis A. Papageorge

Student Name: Mansi Rao Mudrakola

NUID: 002702946

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Part** | **Title** | **Page No.** |
|  |  |  |
| **PART A** | **Security Risk Management Assessment** | **5** |
|  | Exclusive Summary | 6 |
|  | List of Assets with Values ($) | 9 |
|  | List of Threats | 10 |
|  | List of Vulnerabilities | 11 |
|  | Threat/Vulnerability Pairs (with probabilities 0%-100% that a threat will exploit specific vulnerability) | 12 |
|  | Assets impacted by Threat/Vulnerability pairs | 12 |
|  | MOT – which MOT controls are covered by current HGA controls (Histogram) | 14 |
|  | MOT – which MOT controls are covered by current AND proposed by new CISO HGA controls AND VPN server AND DMZ (Histogram) | 15 |
|  | Security Risk Prevention Strategy | 16 |
|  | Security Risk Response (Resilience) Strategy | 29 |
|  | Mixed Security Risk Prevention Strategy and Security Risk Response (Resilience) Strategy | 40 |
|  | Conclusion: Cost Benefit Analysis | 43 |
|  |  |  |
| **PART B** | **Security Risk Management Implementation Plan** | **46** |
|  | Access Control Security Risk Management Implementation Controls and Policies | 47 |
|  | Network Infrastructure Security Risk Management Implementation Controls and Policies | 48 |
|  | Network Infrastructure Management Security Risk Management Implementation Controls and Policies | 48 |
|  | Database Security Risk Management Implementation Controls and Policies | 49 |
|  | Applications Development Security Risk Management Implementation Controls and Policies | 51 |
|  | Wireless Security Risk Management Implementation Controls and Policies | 52 |
|  | List of Cybersecurity Implementation controls that exist at Larsen and Toubro - LTI | 53 |
|  | Comparison of the Implementation controls discussed in class with Larsen and Toubro – LTI’s existing Cybersecurity Implementation controls | 58 |
|  | List of critical assets that exist at Larsen and Toubro - LTI | 64 |
|  | List of potential vulnerabilities for critical assets where Cybersecurity Implementation Controls are missing | 64 |
|  | List of potential threats to Larsen and Toubro - LTI that could exploit vulnerabilities of critical assets | 65 |
|  | List of potential risks for critical assets where Cybersecurity Implementation Controls are missing | 66 |
|  | List of recommended Hardening Prevention controls and policies for each recommended control – Risk Prevention Strategy | 67 |
|  | List of recommended Hardening Response controls and policies for critical assets – Risk Response Strategy | 71 |
|  | Applicable Government Regulations and Industry Standards | 74 |
|  | Rank asset risks and vulnerability risks for Larsen and Toubro -LTI | 77 |
|  | List of Cybersecurity Specialty Areas that exist at Larsen and Toubro -LTI | 80 |
|  | List of Cybersecurity Work Roles that exist at Larsen and Toubro -LTI | 80 |
|  | List of Cybersecurity Tasks that exist at Larsen and Toubro -LTI | 81 |
|  | Comparison of the NCWF recommended Cybersecurity Specialty Areas with Larsen and Toubro -LTI’s existing Cybersecurity Specialty Areas | 88 |
|  | Comparison of the NCWF recommended Cybersecurity Work Roles with Larsen and Toubro -LTI’s existing Cybersecurity Work Roles | 89 |
|  | Comparison the NCWF recommended Cybersecurity Tasks with Larsen and Toubro -LTI’s existing Cybersecurity Tasks | 90 |
|  | List of potential threats to your company that could exploit vulnerabilities of critical assets due to missing Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks | 144 |
|  | List of potential risks for critical assets where Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks are missing | 144 |
|  | List of recommended policies for each recommended Cybersecurity Specialty Area, Cybersecurity Work Role, or Cybersecurity Task that should be created to mitigate the identified risks | 146 |
|  |  |  |
| **PART C** | **Security Risk Management Recommendations** | **148** |
|  | List of Security Risk Prevention and Response Management Recommendations | 149 |
|  | Provide the total cost and benefit in $ | 154 |
|  | Compare proposed security controls, methods and policies budget for HGA with Larsen and Toubro’s controls, methods and policies budget | 156 |
|  | Attack Tree for HGA | 157 |
|  | Attack Tree for Larsen and Toubro – LTI | 158 |
|  | Vulnerabilities and Exploitation Probabilities | 158 |
|  | Cybersecurity workforce recommendations | 160 |
|  |  |  |
| **PART D** | **Appendix** | **161** |
|  | Appendix 3: Detailed Network Topology for HGA | 162 |
|  | Appendix 4: Detailed Network Topology (defense-in-depth) for Larsen and Toubro - LTI | 163 |
|  | References | 165 |

**PART A: Security Risk Management Assessment**

**Executive Summary**

Information System Name: Data-Hypothetical Government Agency

Information System Categorization: Categorizing Assets and rating them using the CIA metrics

|  |  |  |  |
| --- | --- | --- | --- |
| Assets | Metrics | | |
| Confidentiality (C) | Integrity(I) | Availability(A) |
| Financial Resources | High | High | High |
| Systems,Servers,Printers,Routers,Modem Pools | High | High | High |
| Personnel Information | High | High | High |
| Information, Contracting and Compliance Documents | High | High | High |
| Storage Devices and Database | High | High | High |

Organization Name: Hypothetical Government Agency (HGA)

Address: 360 Huntington Ave, Boston, MA 02115

Chandana Lakkaraju

Title: Chief Information Security Officer

Email:chandanalakkaraju@gmail.com

Phone:+19885546403

Sudheer Mudrakola

Title: Information Security Architect

Email:sudheermudrakola@gmail.com

Phone:+19346994853

Srinivas

Title: Information Securiy Analyst

Email:srinivas@gmail.com

Phone:+19052223840

Karthik

Title: Chief Information Officer

Email:karthik@gmail.com

Phone:+17799544615

Information System Operational Status: Fully Operational

Information System Type: Data Management System

Description: Management systems to deal with computer security issues in organizations

System Environment: refer appendix 3

**Interconnection of System Information:**

System Name: Governmental Organization

Type of Organization: A Public Sector Information System

Type of Agreement: Legal Government Contract

Date: May 2,2001

FIPS 199 Category: High

C&A Category: Accredited and Certified

Authorizing Official: Chandana Lakkaraju

**Applicable Laws/Frameworks/Standards/Regulations:**

* ISO 27018 - addresses cloud computing
* ISO 27031 - provides guidance on IT disaster recovery programs and related activities.
* ISO 27040 - addresses storage security.
* NIST SP 800-53 – development of Information Security Frameworks
* COSO – Internal access and controls, frameworks for risk management
* FISMA – maintain an inventory of digital assets, continuous monitoring of IT infrastructure

**Minimum Security Controls:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Control | Observations | Status | `Content Type | Responsible Authority |
| Program Management(M1) | Proper functioning of all levels has been verified | Partial | Common | CIO |
| Risk Management(M2) | Response Teams and Regular analysis reports has been verified | Complete | Common | CISO |
| Life Cycle Planning(M3) | Updation of services and their terms has been completed | Complete | Common | CIO |
| Assurance(M4) | Security systems have been checked | Partial | Common | CIO |
| Incident Reporting and Handling(M5) | Software (SIEM) has been launched into the networks | Complete | Common | CISO |
| Security considerations in support and operations(M6) | List of considerations and operations is in making | Partial | Common | CIO |
| Physical and Environmental Security(M7) | Controls have been verified | Complete | Common | CISO |
| Audit Trails(M8) | Process of identifying areas of failure is in process | Partial | Common | CISO |

Information Security Plan Complete Date: 02/04/2023

Information Security Plan Approval Date: 02/06/2023

The HGA is an organization of 200 employees. The total estimation of the worth of the assets =

$700,000

The total value of the sensitive data and information HGA possesses = $400,000

Asset Valuation:

PC’s = $600\*500 = $300,000

Storage Devices=$500\*300 = $150,000

LAN Server = $90000

Printers = $500\*100 = $50,000

Routers and Modem pools = $400\*250 = $100,000

VPN Server = $5000

DMZ = $50000

**List of Assets with Values ($):**

|  |  |  |
| --- | --- | --- |
| Asset Number | Asset Name | Asset Value |
| A1 | Financial resources | 500000 |
| A2 | PC’s | 300000 |
| A3 | Personnel information | 200000 |
| A4 | Documents | 200000 |
| A5 | Reputation | N/A |
| A6 | Employee confidence | N/A |
| A7 | Storage devices | 150000 |
| A8 | LAN server | 90000 |
| A9 | Printers | 50000 |
| A10 | Routers and Modem pools | 100000 |
| A11 | Console | 50000 |
| A12 | Database | 300000 |
| A13 | VPN Server | 5000 |
| A14 | DMZ | 50000 |

**Selected Subset of Assets:**

|  |  |  |
| --- | --- | --- |
| Asset Number | Asset Name | Asset Value |
| A1 | Financial resources | 500000 |
| A2 | PC’s | 300000 |
| A10 | Routers and Modem pools | 100000 |
| A12 | Database | 300000 |

**List of Threats:**

|  |  |  |
| --- | --- | --- |
| Threat Number | Threat Name | Threat Description |
| T1 | Payroll fraud | Entering false time sheets and modifications of dates |
| T2 | Payroll errors | Receiving duplicate paychecks or using incorrect tax forms |
| T3 | Interruption of Operations | Power outages, connectivity issues, unknown illegal connections |
| T4 | Disclosure of Information | Employees breaking trust and letting out sensitive information of the organization |
| T5 | Insider threats | Accidental modifications/deletion of files and documents |
| T6 | Outsider threats | Unauthorized parties penetrating systems, breaking confidentiality and integrity (stealing data and making changes) |
| T7 | Natural disasters | Fires, floods, storms or other natural events that interrupt regular working of the organization |

**Selected Subset of Threats:**

|  |  |  |
| --- | --- | --- |
| Threat Number | Threat Name | Threat Description |
| T3 | Interruption of Operations | Power outages, connectivity issues, unknown illegal connections |
| T4 | Disclosure of Information | Employees breaking trust and letting out sensitive information of the organization |
| T5 | Insider threats | Accidental modifications/deletion of files and documents |
| T6 | Outsider threats | Unauthorized parties penetrating systems, breaking confidentiality and integrity (stealing data and making changes) |

**List of Vulnerabilities:**

|  |  |
| --- | --- |
| Vulnerability Number | Vulnerability Description |
| V1 | False Time and Attendance Data sheets |
| V2 | Unknown Modifications/Destruction of Payroll Data |
| V3 | Outdated software (lack of assurance due to improper authentication and encryption systems) |
| V4 | Information disclosure |
| V5 | Relay points (microwave stations/satellites) |
| V6 | Improper policies and regulations |
| V7 | Failing to comply with the established standards |

**Selected Subset of Vulnerabilities:**

|  |  |
| --- | --- |
| Vulnerability Number | Vulnerability Description |
| V1 | False Time and Attendance Data sheets |
| V2 | Unknown Modifications/Destruction of Payroll Data |
| V3 | Outdated/Slow software(lack of assurance due to improper authentication and encryption systems) |
| V4 | Information disclosure |

**Threat/Vulnerability Pairs:**

Threat-vulnerability pairs and their likelihood probabilities:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | Total Threat |
| V1 affects A1, A12 | 85 | 85 | 95 | 90 | 355 |
| V2 affects A1, A12 | 85 | 85 | 90 | 95 | 355 |
| V3 affects A1,A2,A10,A12 | 90 | 0 | 0 | 95 | 185 |
| V4 affects A1,A2,A10,A12 | 90 | 98 | 0 | 98 | 286 |

**Asset impacted by Threat/vulnerability pairs:**

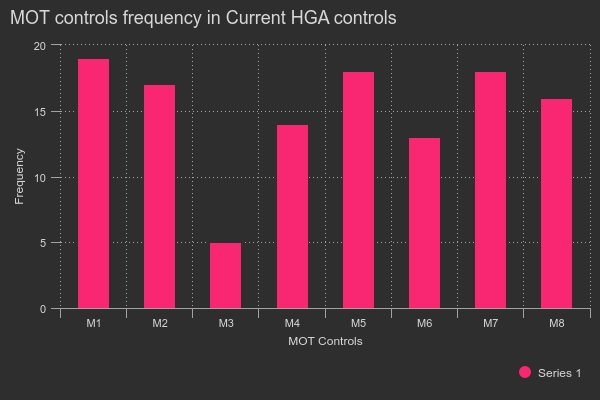
|  |  |
| --- | --- |
| Asset | Vulnerability |
| A1 - Financial resources | V2 - Unknown Modifications/Destruction of Payroll Data |
| V3 - Outdated/Slow software: lack of assurance due to improper authentication and encryption systems |
| V4 - Information disclosure |
| A2 - PC’s | V1 - False Time and Attendance Data sheets |
| V2 - Unknown Modifications/Destruction of Payroll Data |
| V3 - Outdated/Slow software: lack of assurance due to improper authentication and encryption systems |
| V4 - Information disclosure |
| A10 – Routers and Modem Pools | V3 - Outdated/Slow software: lack of assurance due to improper authentication and encryption systems |
| V4 - Information disclosure |
| A12 - Database | V1 - False Time and Attendance Data sheets |
| V2 - Unknown Modifications/Destruction of Payroll Data |
| V3 - Outdated/Slow software: lack of assurance due to improper authentication and encryption systems |
| V4 - Information disclosure |

**MOT Controls**

|  |  |  |
| --- | --- | --- |
| **Management** | **Operational** | **Technical** |
| Program Management(M1) | Incident Reporting and Handling(M5) | Audit Trails(M8) |
| Risk Management(M2) | Security considerations in support and operations(M6) |  |
| Life Cycle Planning(M3) | Physical and Environmental Security(M7) |  |
| Assurance(M4) |  |  |

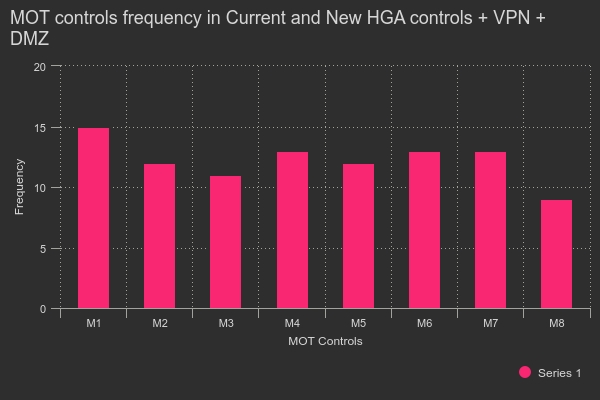
**List of current security controls and policies with MOT controls**

|  |  |  |  |
| --- | --- | --- | --- |
| Control and Policy Category | Current Security Control and Policy (CSCP) number | Control and Policy Description | MOT controls |
| General use of HGA Computer Systems | CSCP1 | Computer Operations Group (COG) rules and responsibilities | 2,5,6,8 |
| CSCP2 | Security Awareness and Training sessions | 1,2,5,7 |
| CSCP3 | Proper documentations | 2,3,4,5,6 |
| CSCP4 | Allowance of only authorized access | 1,2,5,6,7,8 |
| CSCP5 | Comply to the policies and procedures | 4,7 |
| CSCP6 | Access control | 1,2,5,6,7,8 |
| Payroll Frauds and Errors | CSCP7 | Comply to the Privacy Act | 4,7 |
| CSCP8 | Verification of time and attendance data | 1,4,5,7,8 |
| CSCP9 | Prevention of destruction/modification of data | 1,4,5,7,8 |
| CSCP10 | Protection against payroll errors | 1,4,7,8 |
| CSCP11 | Protection against unauthorized execution of data | 1,2,5,6,7,8 |
| Interruptions of Operations | CSCP12 | Contingency Planning | 1,2,3,4,5,6 |
| CSCP13 | Division contingency planning | 1,3,4,8 |
| Information Disclosure | CSCP14 | Need-to-know policy | 1,2,4,8 |
| CSCP15 | Appropriate screening and hiring | 1,2,5,7 |
| CSCP16 | Proper documentations and their security | 1,2,3,4,5,6,7,8 |
| CSCP17 | Access control mechanisms | 1,2,5,6,7,8 |
| CSCP18 | Training and security awareness | 1,2,5,7 |
| Network Security | CSCP19 | Restrict interactions and permissions | 1,2,5,6,7,8 |
| CSCP20 | Router configurations | 1,2,4,5,6,7,8 |
| CSCP21 | LAN configurations | 1,2,4,5,6,7,8 |
| Non-HGA ComputerSystems | CSCP22 | Information disclosure policy | 1,2,4,5,6,7,8 |
| CSCP23 | Written commitment grants | 1,2,3,4,5,6,7,8 |



**New Security policies recommended by the CISO and Team members**

|  |  |  |  |
| --- | --- | --- | --- |
| Control and Policy Category | New Security Policy (NSP) number | Control and Policy Description | MOT controls |
| Payroll Fraud Vulnerabilities | NSP1 | Strong authentication mechanisms (OTP’s or MFA) | 1,2,5,6,7,8 |
| NSP2 | Improving server’s administrative procedures | 1,2,3,4,5,6,7,8 |
| NSP3 | Smart authentication division systems | 1,3,4,8 |
| Payroll Error Vulnerabilities | NSP4 | Compliance incentives and penalties | 1,4,5,6,7 |
| NSP5 | Paperwork and reports | 1,2,3,4,5,6,7,8 |
| Continuity of Operation Vulnerabilities | NSP6 | Additional contingency training | 1,2,3,4,5,6 |
| NSP7 | Backup facilities | 1,2,3,4,5,6,7,8 |
| NSP8 | Reviewing policies and making corrections | 1,3,6,7 |
| NSP9 | Improve virus-prevention mechanisms | 1,2,3,4,5,6,8 |
| Information Disclosure | NSP10 | Compliance audits | 1,2,3,4,5,6,7,8 |
| NSP11 | Screen lock policies | 1,3,4,7 |
| NSP12 | Modifying storage and backup | 1,2,3,4,7 |
| Network Related Vulnerabilities | NSP13 | Strengthen IAM | 1,2,5,6,7,8 |
| NSP14 | Encryptions to modem pools and server-to-mainframe communications | 1,2,4,5,6,7,8 |
| NSP15 | VPN | 2,3,4,5,6,7 |
| NSP16 | DMZ | 1,2,4,5,6,7 |



**Security Risk Prevention Strategy**

**Security Risk ($) Calculations of Assets with vulnerabilities discovered by new CISO and protected by implementing the proposed controls by new CISO, missing MOT controls, and Demilitarized Zone (DMZ) and Virtual Private Network (VPN). Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking which vulnerability could still be addressed, thus further reducing HGA’s residual risk. 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**

**Selected Subset of Assets:**

|  |  |  |
| --- | --- | --- |
| Asset Number | Asset Name | Asset Value |
| A1 | Financial resources | 500000 |
| A2 | PC’s | 300000 |
| A10 | Routers and Modem pools | 100000 |
| A12 | Database | 300000 |

**Selected Subset of Threats:**

|  |  |  |
| --- | --- | --- |
| Threat Number | Threat Name | Threat Description |
| T3 | Interruption of Operations | Power outages, connectivity issues, unknown illegal connections |
| T4 | Disclosure of Information | Employees breaking trust and letting out sensitive information of the organization |
| T5 | Insider threats | Accidental modifications/deletion of files and documents |
| T6 | Outsider threats | Unauthorized parties penetrating systems, breaking confidentiality and integrity (stealing data and making changes) |

**Selected Subset of Vulnerabilities:**

|  |  |
| --- | --- |
| Vulnerability Number | Vulnerability Description |
| V1 | False Time and Attendance Data sheets |
| V2 | Unknown Modifications/Destruction of Payroll Data |
| V3 | Outdated/Slow software(lack of assurance due to improper authentication and encryption systems) |
| V4 | Information disclosure |

Threat-vulnerability pairs and their likelihood probabilities:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | Total Threat |
| V1 affects A1, A12 | 85 | 85 | 95 | 90 | 355 |
| V2 affects A1, A12 | 85 | 85 | 90 | 95 | 355 |
| V3 affects A1,A2,A10,A12 | 90 | 0 | 0 | 95 | 185 |
| V4 affects A1,A2,A10,A12 | 90 | 98 | 0 | 98 | 286 |

The probability table of threat exploiting vulnerability will be as:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Likelihood of Threat exploiting the vulnerability | | | | | | | | | | | | | | | |
| Asset | T3\*V1 | T3\*V2 | T3\*V3 | T3\*V4 | T4\*V1 | T4\*V2 | T4\*V3 | T4\*V4 | T5\*V1 | T5\*V2 | T5\*V3 | T5\*V4 | T6\*V1 | T6\*V2 | T6\*V3 | T6\*V4 |
| A1 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A2 | 0 | 0 | 100 | 100 | 0 | 0 | 100 | 100 | 0 | 0 | 100 | 100 | 0 | 0 | 100 | 100 |
| A10 | 0 | 0 | 100 | 100 | 0 | 0 | 100 | 100 | 0 | 0 | 100 | 100 | 0 | 0 | 100 | 100 |
| A12 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |

**Residual Asset Security Risks Calculation**

Residual Asset Security Risk = Inherent Risk

= Asset Value\* Sum(Subset(T(i)\*V(i))) of respective asset only

Residual Asset Security Risk Table:

|  |  |  |  |
| --- | --- | --- | --- |
| Asset number | Asset Value | Sum(Subset(T(i)\*V(i))) of respective asset only | (Residual Asset Security Risk = (Asset Value\*Sum(Subset(T(i)\*V(i))) of respective asset only)/100 |
| A1 | 500000 | 1181 | 5,905,000 |
| A2 | 300000 | 471 | 1,413,000 |
| A10 | 100000 | 471 | 471,000 |
| A12 | 300000 | 1181 | 3,543,000 |

**Vulnerability Security Risk Calculation**

Vulnerability Security Risk = ∑ (Each Asset Value\*Each Vulnerability’s total threat)/100

V1 = [(500000\*355)+(300000\*355)]/100 = 2840000

V2 = [(500000\*355)+(300000\*355)]/100 = 2840000

V3 = [(500000\*185)+(300000\*185)+(100000\*185)+(300000\*185)]/100 = 2220000

V4 = [(500000\*286)+(300000\*286)+(100000\*286)+(300000\*286)]/100 = 3432000

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A1 | 5,905,000 | 1 |
| A12 | 3,543,000 | 2 |
| A2 | 1,413,000 | 3 |
| A10 | 471,000 | 4 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V4 | 3432000 | 1 |
| V2 | 2840000 | 2 |
| V1 | 2840000 | 3 |
| V3 | 2220000 | 4 |

**Security Risk Prevention Strategy P1**

In the HGA case study, most of the Security controls have been implemented in current and new CISO proposed rules, a few of the missing ones are in the table below. These current, new security controls and MOT controls altogether help in reducing the probabilities of impact to major extent.

**List of Missing MOT Controls:**

|  |  |  |
| --- | --- | --- |
| **Management** | **Operational** | **Technical** |
| Program Management(M1) | Incident Reporting and Handling(M5) | Audit Trails(M8) |
| Risk Management(M2) | Security considerations in support and operations(M6) |  |
| Life Cycle Planning(M3) | Physical and Environmental Security(M7) |  |
| Assurance(M4) |  |  |

The HGA Management has added two new asset to the whole security infrastructure – The Virtual Private Network (VPN) and the Demilitarized Zone (DMZ). A VPN provides effective secure the network. It provides secure access without the maintenance and cost of expensive routing hardware and in addition to it, it creates a secure connection between user devices and network or other resources they long into thus benefitting the enterprise. A DMZ refers to a subnet that is physically or logically separated from internal network and is used to separate untrusted devices from trusted devices. A DMZ adds an extra layer of security to prevent an attacker from getting into system.

Costs:

VPN Server = $5000

DMZ = $50000

**Updated Subset of Assets**

|  |  |  |
| --- | --- | --- |
| Asset Number | Asset Name | Asset Value |
| A1 | Financial resources | 500000 |
| A2 | PC’s | 300000 |
| A10 | Routers and Modem pools | 100000 |
| A12 | Database | 300000 |
| A13 | VPN Server | 5000 |
| A14 | DMZ | 50000 |

**Updated Subset of Threats**

|  |  |  |
| --- | --- | --- |
| Threat Number | Threat Name | Threat Description |
| T3 | Interruption of Operations | Power outages, connectivity issues, unknown illegal connections |
| T4 | Disclosure of Information | Employees breaking trust and letting out sensitive information of the organization |
| T5 | Insider threats | Accidental modifications/deletion of files and documents |
| T6 | Outsider threats | Unauthorized parties penetrating systems, breaking confidentiality and integrity (stealing data and making changes) |
| T7 | Natural disasters | Fires, floods, storms or other natural events that interrupt regular working of the organization |

**Updated Subset of Vulnerabilities**

|  |  |
| --- | --- |
| Vulnerability Number | Vulnerability Description |
| V1 | False Time and Attendance Data sheets |
| V2 | Unknown Modifications/Destruction of Payroll Data |
| V3 | Outdated/Slow software (lack of assurance due to improper authentication and encryption systems) |
| V4 | Information disclosure |
| V5 | Relay points (microwave stations/satellites) |

Threat-vulnerability pairs and their updated likelihood probabilities:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | T7 | Total Threat |
| V1 affects A1, A12 | 30 | 30 | 45 | 40 | 0 | 145 |
| V2 affects A1, A12 | 30 | 30 | 40 | 45 | 0 | 145 |
| V3 affects A1,A2,A10,A12,A14 | 40 | 0 | 0 | 45 | 0 | 85 |
| V4 affects A1,A2,A10,A12,A13,A14 | 40 | 48 | 0 | 48 | 0 | 136 |
| V5 affects A1,A2,A10,A12,A13,A14 | 40 | 35 | 20 | 30 | 40 | 165 |

The probability table of threat exploiting vulnerability will be as:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Likelihood of Threat exploiting the vulnerability | | | | | | | | | | | | | | | | | | | | | | | | |
| Asset | T3\*V1 | T3\*V2 | T3\*V3 | T3\*V4 | T3\*V5 | T4\*V1 | T4\*V2 | T4\*V3 | T4\*V4 | T4\*V5 | T5\*V1 | T5\*V2 | T5\*V3 | T5\*V4 | T5\*V5 | T6\*V1 | T6\*V2 | T6\*V3 | T6\*V4 | T6\*V5 | T7\*V1 | T7\*V2 | T7\*V3 | T7\*V4 | T7\*V5 |
| A1 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 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 | 50 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A10 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A12 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A13 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A14 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |

Residual Asset Security Risk = Inherent Risk = Asset Value\*Sum(Subset(T(i)\*V(i))) of respective asset only

**Residual Asset Security Risk Table and Calculation**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset number | Asset Value | Sum(Subset(T(i)\*V(i))) of respective asset only | (Residual Asset Security Risk = (Asset Value\*Sum(Subset(T(i)\*V(i))) of respective asset only)/100 |
| A1 | 500000 | 676 | 3380000 |
| A2 | 300000 | 386 | 1158000 |
| A10 | 100000 | 386 | 386000 |
| A12 | 300000 | 676 | 2028000 |
| A13 | 5000 | 301 | 15050 |
| A14 | 50000 | 386 | 193000 |

**Vulnerability Security Risk Calculation**

Vulnerability Security Risk = ∑(Asset Value\*Each Vulnerability’s total threat)/100

V1 = [(500000\*145)+(300000\*145)]/100 = 1160000

V2 = [(500000\*145)+(300000\*145)]/100 = 1160000

V3 = [(500000\*85)+(300000\*85)+(100000\*85)+(300000\*85)+(50000\*85)]/100 = 1062500

V4 = [(500000\*136)+(300000\*136)+(100000\*136)+(300000\*136)+(5000\*136)+(50000\*136)]/100 = 1706800

V5 = [(500000\*165)+(300000\*165)+(100000\*165)+(300000\*165)+(5000\*165)+(50000\*165)]/100 = 2070750

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A1 | 3380000 | 1 |
| A12 | 2028000 | 2 |
| A2 | 1158000 | 3 |
| A10 | 386000 | 4 |
| A14 | 193000 | 5 |
| A13 | 15050 | 6 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V5 | 2070750 | 1 |
| V4 | 1706800 | 2 |
| V2 | 1160000 | 3 |
| V1 | 1160000 | 4 |
| V3 | 1062500 | 5 |

**Security Risk Prevention Strategy P2**

Applied additional Hardening Controls to highest ranked Vulnerability Risk, with further reduced probabilities, thus further reducing the overall security asset residual risk and create a new ranking of vulnerability security risks. In this step you may need to include in the Asset inventory the value of points from the M-O-T Controls AND DMZ and VPN in Step P1.

The **Vulnerability V5:** **Relay points (microwave stations/satellites)** is a vulnerability which the highest ranked and poses danger. This effect can be reduced by forming networks which depend less on relay points and use their services only when it is necessary. The lesser the number of such relay points the better the network. We can also include strong encryption systems to all the relay points to further decrease the effect of this vulnerability.

Threat-vulnerability pairs and their updated likelihood probabilities:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | T7 | Total Threat |
| V1 affects A1, A12 | 30 | 30 | 45 | 40 | 0 | 145 |
| V2 affects A1, A12 | 30 | 30 | 40 | 45 | 0 | 145 |
| V3 affects A1,A2,A10,A12,A14 | 40 | 0 | 0 | 45 | 0 | 85 |
| V4 affects A1,A2,A10,A12,A13,A14 | 40 | 48 | 0 | 48 | 0 | 136 |
| **V5 affects A1,A2,A10,A12,A13,A14** | **4** | **10** | **6** | **8** | **5** | **33** |

The probability table of threat exploiting vulnerability will be as:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Likelihood of Threat exploiting the vulnerability | | | | | | | | | | | | | | | | | | | | | | | | |
| Asset | T3\*V1 | T3\*V2 | T3\*V3 | T3\*V4 | T3\*V5 | T4\*V1 | T4\*V2 | T4\*V3 | T4\*V4 | T4\*V5 | T5\*V1 | T5\*V2 | T5\*V3 | T5\*V4 | T5\*V5 | T6\*V1 | T6\*V2 | T6\*V3 | T6\*V4 | T6\*V5 | T7\*V1 | T7\*V2 | T7\*V3 | T7\*V4 | T7\*V5 |
| A1 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 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 | 50 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A10 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A12 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A13 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |
| A14 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 |

Residual Asset Security Risk = Inherent Risk = Asset Value\*Sum(Subset(T(i)\*V(i))) of respective asset only

**Residual Asset Security Risk Table and Calculations**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset number | Asset Value | Sum(Subset(T(i)\*V(i))) of respective asset only | (Residual Asset Security Risk = (Asset Value\*Sum(Subset(T(i)\*V(i))) of respective asset only)/100 |
| A1 | 500000 | 544 | 2720000 |
| A2 | 300000 | 254 | 762000 |
| A10 | 100000 | 254 | 254000 |
| A12 | 300000 | 544 | 1632000 |
| A13 | 5000 | 169 | 8450 |
| A14 | 50000 | 254 | 127000 |

**Vulnerability Security Risk Calculation**

Vulnerability Security Risk = ∑(Asset Value\*Each Vulnerability’s total threat)/100

V1 = [(500000\*145)+(300000\*145)]/100 = 1160000

V2 = [(500000\*145)+(300000\*145)]/100 = 1160000

V3 = [(500000\*85)+(300000\*85)+(100000\*85)+(300000\*85)+(50000\*85)]/100 = 1062500

V4 = [(500000\*136)+(300000\*136)+(100000\*136)+(300000\*136)+(5000\*136)+(50000\*136)]/100 = 1706800

**V5 = [(500000\*33)+(300000\*33)+(100000\*33)+(300000\*33)+(5000\*33)+(50000\*33)]/100 = 414150**

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A1 | 2720000 | 1 |
| A12 | 1632000 | 2 |
| A2 | 762000 | 3 |
| A10 | 254000 | 4 |
| A14 | 127000 | 5 |
| A13 | 8450 | 6 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V4 | 1706800 | 1 |
| V2 | 1160000 | 2 |
| V1 | 1160000 | 3 |
| V3 | 1062500 | 4 |
| **V5** | **414150** | **5** |

**Security Risk Prevention Strategy P3**

Applied additional Hardening Controls to new now highest ranked Vulnerability Risk, thus further reducing the security asset residual risks and create a new ranking of vulnerability security risks. In this step you may need to include in the Asset inventory the value of points from the M-O-T Controls in Step P2.

The **Vulnerability V4: Information disclosure** is the highest ranked vulnerability and poses danger. And therefore, the organization should try limiting the access to the employees and allow access to only data that is to be worked on by the employee. The organization needs to be sure of the employee before giving in any highly confidential data. Trusting an employee by the duration of work and experience can be a wrong conclusion sometimes.

Thus, the threat-vulnerability pair table and the updated likelihood probabilities for Vulnerability V1 will be:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | T7 | Total Threat |
| V1 affects A1, A12 | 30 | 30 | 45 | 40 | 0 | 145 |
| V2 affects A1, A12 | 30 | 30 | 40 | 45 | 0 | 145 |
| V3 affects A1,A2,A10,A12,A14 | 40 | 0 | 0 | 45 | 0 | 85 |
| **V4 affects A1,A2,A10,A12,A13,A14** | **5** | **8** | **0** | **6** | **0** | **19** |
| V5 affects A1,A2,A10,A12,A13,A14 | 4 | 10 | 6 | 8 | 5 | 33 |

Residual Asset Security Risk = Inherent Risk = Asset Value\*Sum(Subset(T(i)\*V(i))) of respective asset only

**Residual Asset Security Risk Table and Calculations**

|  |  |  |  |
| --- | --- | --- | --- |
| Asset number | Asset Value | Sum(Subset(T(i)\*V(i))) of respective asset only | (Residual Asset Security Risk = (Asset Value\*Sum(Subset(T(i)\*V(i))) of respective asset only)/100 |
| A1 | 500000 | 427 | 2135000 |
| A2 | 300000 | 137 | 411000 |
| A10 | 100000 | 137 | 137000 |
| A12 | 300000 | 427 | 1281000 |
| A13 | 5000 | 52 | 2600 |
| A14 | 50000 | 137 | 68500 |

**Vulnerability Security Risk Calculation**

Vulnerability Security Risk = ∑(Asset Value\*Each Vulnerability’s total threat)/100

V1 = [(500000\*145)+(300000\*145)]/100 = 1160000

V2 = [(500000\*145)+(300000\*145)]/100 = 1160000

V3 = [(500000\*85)+(300000\*85)+(100000\*85)+(300000\*85)+(50000\*85)]/100 = 1062500

**V4 = [(500000\*19)+(300000\*19)+(100000\*19)+(300000\*19)+(5000\*19)+(50000\*19)]/100 = 238450**

V5 = [(500000\*33)+(300000\*33)+(100000\*33)+(300000\*33)+(5000\*33)+(50000\*33)]/100 = 414150

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A1 | 2135000 | 1 |
| A12 | 1281000 | 2 |
| A2 | 411000 | 3 |
| A10 | 137000 | 4 |
| A14 | 68500 | 5 |
| A13 | 2600 | 6 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V2 | 1160000 | 1 |
| V1 | 1160000 | 2 |
| V3 | 1062500 | 3 |
| V5 | 414150 | 4 |
| **V4** | **238450** | **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.**

The HGA controls listed were further strengthened by the controls proposed by the CISO and the team. Additionally, MOT(Management-Operational-Technical) controls and VPN plus DMZ controls were added to ensure an overall secure infrastructure. Even after such strong controls have been included in the strategy, a few more could be added and this information could be obtained through the understanding of Common Criteria(CC). CC is a framework that allows employees of organizations who tend to be the users to specify security requirements.

According to CC, the CISO and team could focus on classification of devices and accordingly make “Protection Profiles” which are documents stating security policies for that particular set of devices. It could also ensure the validity of the compliance audits through establishment of the Evaluation Assurance Level (EAL), which is a rating standard that describes the depth and correctness of the evaluation.

**Security Risk Response (Resilience) Strategy**

**Use threat/vulnerability pairs with probabilities from XI above and apply Hardening Controls to highest ranked Residual Asset Risk, thus reducing Risk Impact probabilities, and further reducing the overall security asset residual risk. Calculate residual risks for assets and total HGA residual risk. Provide a ranking for which risk impacts could still be addressed, thus further reducing HGA’s residual risk. Compare the list of current HGA controls plus CISO proposed response controls plus missing MOT response controls plus VPN plus DMZ risk controls to the 157 risk controls from Common Criteria.**

In the HGA case study, most of the Security controls have been implemented in current and new CISO proposed rules, a few of the missing ones are in the table below. These current, new security controls and MOT controls altogether help in reducing the probabilities of impact to major extent.

|  |  |  |
| --- | --- | --- |
| **Management** | **Operational** | **Technical** |
| Program Management(M1) | Incident Reporting and Handling(M5) | Audit Trails(M8) |
| Risk Management(M2) | Security considerations in support and operations(M6) |  |
| Life Cycle Planning(M3) | Physical and Environmental Security(M7) |  |
| Assurance(M4) |  |  |

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

Threat-vulnerability pairs and their updated likelihood probabilities:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | T7 | Total Threat |
| V1 affects A1, A12 | 30 | 30 | 45 | 40 | 0 | 145 |
| V2 affects A1, A12 | 30 | 30 | 40 | 45 | 0 | 145 |
| V3 affects A1,A2,A10,A12,A14 | 40 | 0 | 0 | 45 | 0 | 85 |
| V4 affects A1,A2,A10,A12,A13,A14 | 5 | 8 | 0 | 6 | 0 | 19 |
| V5 affects A1,A2,A10,A12,A13,A14 | 4 | 10 | 6 | 8 | 5 | 33 |

The probability table of threat exploiting vulnerability will be updated as:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Likelihood of Threat exploiting the vulnerability | | | | | | | | | | | | | | | | | | | | | | | | |
| Asset | T3\*V1 | T3\*V2 | T3\*V3 | T3\*V4 | T3\*V5 | T4\*V1 | T4\*V2 | T4\*V3 | T4\*V4 | T4\*V5 | T5\*V1 | T5\*V2 | T5\*V3 | T5\*V4 | T5\*V5 | T6\*V1 | T6\*V2 | T6\*V3 | T6\*V4 | T6\*V5 | T7\*V1 | T7\*V2 | T7\*V3 | T7\*V4 | T7\*V5 |
| A1 | 30 | 20 | 60 | 40 | 40 | 60 | 30 | 30 | 20 | 30 | 50 | 50 | 30 | 20 | 20 | 50 | 60 | 30 | 30 | 40 | 10 | 20 | 10 | 10 | 40 |
| A2 | 0 | 0 | 50 | 50 | 40 | 0 | 0 | 50 | 40 | 40 | 0 | 0 | 40 | 50 | 50 | 0 | 0 | 70 | 50 | 60 | 0 | 0 | 20 | 10 | 50 |
| A10 | 0 | 0 | 40 | 30 | 40 | 0 | 0 | 20 | 60 | 40 | 0 | 0 | 60 | 60 | 50 | 0 | 0 | 50 | 60 | 50 | 0 | 0 | 10 | 20 | 40 |
| A12 | 50 | 30 | 20 | 20 | 50 | 20 | 20 | 60 | 30 | 50 | 30 | 20 | 50 | 20 | 60 | 30 | 20 | 20 | 40 | 60 | 20 | 20 | 10 | 10 | 20 |
| A13 | 0 | 0 | 0 | 30 | 40 | 0 | 0 | 0 | 60 | 50 | 0 | 0 | 0 | 50 | 40 | 0 | 0 | 0 | 60 | 50 | 0 | 0 | 0 | 30 | 20 |
| A14 | 0 | 0 | 30 | 30 | 40 | 0 | 0 | 20 | 30 | 40 | 0 | 0 | 20 | 30 | 30 | 0 | 0 | 30 | 50 | 50 | 0 | 0 | 20 | 30 | 30 |

**Calculations for Residual Asset Security Risk**

Asset A1 Risk = (500000\*((30\*30)+(30\*20)+(40\*60)+(5\*40)+(4\*40)+(30\*60)+(30\*30)+(0\*30)+(8\*20)+(10\*30)+(45\*50)+(40\*50)+(0\*30)+(0\*20)+(6\*20)+(40\*50)+(45\*60)+(45\*30)+(6\*30)+(8\*40)+(0\*10)+(0\*20)+(0\*10)+(0\*10)+(5\*40)))/10000 = **927000**

Asset A2 Risk =

(300000\*((40\*50)+(5\*50)+(4\*40)+(0\*50)+(8\*40)+(10\*40)+(0\*40)+(0\*50)+(6\*50)+(45\*70)+(6\*50)+(8\*60)+(0\*20)+(0\*10)+(5\*50)))/ 10000 = **228300**

Asset A10 Risk =

(100000\*((40\*40)+(5\*30)+(4\*40)+(0\*20)+(8\*60)+(10\*40)+(0\*60)+(0\*60)+(6\*50)+(45\*50)+(6\*60)+(8\*50)+(0\*10)+(0\*20)+(5\*40)))/ 10000 = **63000**

Asset A12 Risk =

(300000\*((30\*50)+(30\*30)+(40\*20)+(5\*20)+(4\*50)+(30\*20)+(30\*20)+(0\*60)+(8\*30)+(10\*50)+(45\*30)+(40\*20)+(0\*50)+(0\*20)+(6\*60)+(40\*30)+(45\*20)+(45\*20)+(6\*40)+(8\*60)+(0\*20)+(0\*20)+(0\*10)+(0\*10)+(5\*20)))/10000 = **353100**

Asset A13 Risk =

(5000\*((5\*30)+(4\*40)+(8\*60)+(10\*50)+(0\*50)+(6\*40)+(6\*60)+(8\*50)+(0\*30)+(5\*20)))/ 10000 = **1195**

Asset A14 Risk =

(50000\*((40\*30)+(5\*30)+(4\*40)+(0\*20)+(8\*30)+(10\*40)+(0\*20)+(0\*30)+(6\*30)+(45\*30)+(6\*50)+(8\*50)+(0\*20)+(0\*30)+(5\*30)))/ 10000 =**22650**

**Calculations for Residual Vulnerability Security Risk**

Risk due to V1 = ((500000\*((30\*30)+(30\*60)+(45\*50)+(40\*50)+(0\*10))+(300000\*((30\*50)+(30\*20)+(45\*30)+(40\*30)+(0\*20)))/10000 = **487000**

Risk due to V2 = ((500000\*((30\*20)+(30\*30)+(40\*50)+(45\*60)+(0\*20)))+(300000\*((30\*30)+(30\*20)+(40\*20)+(45\*20)+(0\*20))))/10000 = **406000**

Risk due to V3 =

((500000\*((40\*60)+(0\*30)+(0\*30)+(45\*30)+(0\*10)))+(300000\*((40\*50)+(0\*50)+(0\*40)+(45\*70)+(0\*20)))+(100000\*((40\*40)+(0\*20)+(0\*60)+(45\*50)+(0\*10)))+(300000\*((40\*20)+(0\*60)+(0\*50)+(45\*20)+(0\*10)))+(50000\*((4\*30)+(0\*20)+(0\*20)+(45\*30)+(0\*20))))/10000 = **438850**

Risk due to V4 =

((500000\*((5\*40)+(8\*20)+(0\*20)+(6\*30)+(0\*10)))+(300000\*((5\*50)+(8\*40)+(0\*50)+(6\*50)+(0\*10)))+(100000\*((5\*30)+(8\*60)+(0\*60)+(6\*60)+(0\*20)))+(300000\*((5\*20)+(8\*30)+(0\*20)+(6\*40)+(0\*10)))+(5000\*((5\*30)+(8\*60)+(0\*50)+(6\*60)+(0\*30)))+(50000\*((5\*40)+(8\*40)+(0\*30)+(6\*50)+(0\*30))))/10000 = **384345**

Risk due to V5 =

((500000\*((4\*40)+(10\*30)+(6\*20)+(8\*40)+(5\*40)))+(300000\*((4\*40)+(10\*40)+(6\*50)+(8\*60)+(5\*50)))+(100000\*((4\*40)+(10\*40)+(6\*50)+(8\*50)+(5\*40)))+(300000\*((4\*50)+(10\*50)+(6\*60)+(8\*60)+(5\*20)))+(5000\*((4\*40)+(10\*50)+(6\*40)+(8\*50)+(5\*20)))+(50000\*((4\*30)+(10\*30)+(6\*30)+(8\*50)+(5\*30))))/10000 = **172950**

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A1 | 927000 | 1 |
| A12 | 353100 | 2 |
| A2 | 228300 | 3 |
| A10 | 63000 | 4 |
| A14 | 22650 | 5 |
| A13 | 1195 | 6 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V1 | 487000 | 1 |
| V3 | 438850 | 2 |
| V2 | 406000 | 3 |
| V4 | 384345 | 4 |
| V5 | 172950 | 5 |

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

Applied additional Hardening Controls (for example restricting services or adding a redundant server) to highest ranked Residual Asset Risk, thus further reducing risk impact probabilities, and further reduced the overall security asset residual risk and created a new ranking of vulnerability security risks. In this step we’ve included the value of points from the M-O-T Controls in Step R1 if the value of controls is comparable to value of Critical Assets.

**From R1, the Highest ranked asset is A1 for its risk**. Financial resources of an organization are the most important assets. Budget, costs and expenses and all the salary and payroll data define and are the basis of any organization. These can be at high risk and therefore to reduce the threat to this asset controls such as the following can be taken : maintaining strict confidentiality, provide physical security to documents and having strong encryption and authentication measures to all the devices in the network that contain financial documents and data.

Thus, applying the controls on P3 table, the threat-vulnerability pair table with the updated likelihood probabilities will be:

Threat-vulnerability pairs and their updated likelihood probabilities:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | T7 | Total Threat |
| V1 affects A1, A12 | 30 | 30 | 45 | 40 | 0 | 145 |
| V2 affects A1, A12 | 30 | 30 | 40 | 45 | 0 | 145 |
| V3 affects A1,A2,A10,A12,A14 | 40 | 0 | 0 | 45 | 0 | 85 |
| V4 affects A1,A2,A10,A12,A13,A14 | 5 | 8 | 0 | 6 | 0 | 19 |
| V5 affects A1,A2,A10,A12,A13,A14 | 4 | 10 | 6 | 8 | 5 | 33 |

The probability table of threat exploiting vulnerability will be updated as:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Likelihood of Threat exploiting the vulnerability | | | | | | | | | | | | | | | | | | | | | | | | |
| Asset | T3\*V1 | T3\*V2 | T3\*V3 | T3\*V4 | T3\*V5 | T4\*V1 | T4\*V2 | T4\*V3 | T4\*V4 | T4\*V5 | T5\*V1 | T5\*V2 | T5\*V3 | T5\*V4 | T5\*V5 | T6\*V1 | T6\*V2 | T6\*V3 | T6\*V4 | T6\*V5 | T7\*V1 | T7\*V2 | T7\*V3 | T7\*V4 | T7\*V5 |
| **A1** | **3** | **2** | **6** | **4** | **4** | **6** | **3** | **3** | **2** | **3** | **5** | **5** | **3** | **2** | **2** | **5** | **6** | **3** | **3** | **4** | **1** | **2** | **1** | **1** | **4** |
| A2 | 0 | 0 | 50 | 50 | 40 | 0 | 0 | 50 | 40 | 40 | 0 | 0 | 40 | 50 | 50 | 0 | 0 | 70 | 50 | 60 | 0 | 0 | 20 | 10 | 50 |
| A10 | 0 | 0 | 40 | 30 | 40 | 0 | 0 | 20 | 60 | 40 | 0 | 0 | 60 | 60 | 50 | 0 | 0 | 50 | 60 | 50 | 0 | 0 | 10 | 20 | 40 |
| A12 | 50 | 30 | 20 | 20 | 50 | 20 | 20 | 60 | 30 | 50 | 30 | 20 | 50 | 20 | 60 | 30 | 20 | 20 | 40 | 60 | 20 | 20 | 10 | 10 | 20 |
| A13 | 0 | 0 | 0 | 30 | 40 | 0 | 0 | 0 | 60 | 50 | 0 | 0 | 0 | 50 | 40 | 0 | 0 | 0 | 60 | 50 | 0 | 0 | 0 | 30 | 20 |
| A14 | 0 | 0 | 30 | 30 | 40 | 0 | 0 | 20 | 30 | 40 | 0 | 0 | 20 | 30 | 30 | 0 | 0 | 30 | 50 | 50 | 0 | 0 | 20 | 30 | 30 |

**Calculations for Residual Asset Security Risk**

**Asset A1 Risk = (500000\*((30\*3)+(30\*2)+(40\*6)+(5\*4)+(4\*4)+(30\*6)+(30\*3)+(0\*3)+(8\*2)+(10\*3)+(45\*5)+(40\*5)+(0\*3)+(0\*2)+(6\*2)+(40\*5)+(45\*6)+(45\*3)+(6\*3)+(8\*4)+(0\*1)+(0\*2)+(0\*1)+(0\*1)+(5\*4)))/10000 = 92700**

Asset A2 Risk =

(300000\*((40\*50)+(5\*50)+(4\*40)+(0\*50)+(8\*40)+(10\*40)+(0\*40)+(0\*50)+(6\*50)+(45\*70)+(6\*50)+(8\*60)+(0\*20)+(0\*10)+(5\*50)))/ 10000 = **228300**

Asset A10 Risk =

(100000\*((40\*40)+(5\*30)+(4\*40)+(0\*20)+(8\*60)+(10\*40)+(0\*60)+(0\*60)+(6\*50)+(45\*50)+(6\*60)+(8\*50)+(0\*10)+(0\*20)+(5\*40)))/ 10000 = **63000**

Asset A12 Risk =

(300000\*((30\*50)+(30\*30)+(40\*20)+(5\*20)+(4\*50)+(30\*20)+(30\*20)+(0\*60)+(8\*30)+(10\*50)+(45\*30)+(40\*20)+(0\*50)+(0\*20)+(6\*60)+(40\*30)+(45\*20)+(45\*20)+(6\*40)+(8\*60)+(0\*20)+(0\*20)+(0\*10)+(0\*10)+(5\*20)))/10000 = **353100**

Asset A13 Risk =

(5000\*((5\*30)+(4\*40)+(8\*60)+(10\*50)+(0\*50)+(6\*40)+(6\*60)+(8\*50)+(0\*30)+(5\*20)))/ 10000 = **1195**

Asset A14 Risk =

(50000\*((40\*30)+(5\*30)+(4\*40)+(0\*20)+(8\*30)+(10\*40)+(0\*20)+(0\*30)+(6\*30)+(45\*30)+(6\*50)+(8\*50)+(0\*20)+(0\*30)+(5\*30)))/ 10000 =**22650**

**Calculations for Residual Vulnerability Security Risk**

Risk due to V1 = ((500000\*((30\*3)+(30\*6)+(45\*5)+(40\*5)+(0\*1))+(300000\*((30\*50)+(30\*20)+(45\*30)+(40\*30)+(0\*20)))))/10000 = **174250**

Risk due to V2 = ((500000\*((30\*2)+(30\*3)+(40\*5)+(45\*6)+(0\*2)))+(300000\*((30\*30)+(30\*20)+(40\*20)+(45\*20)+(0\*20))))/10000 = **127000**

Risk due to V3 =

((500000\*((40\*6)+(0\*3)+(0\*3)+(45\*3)+(0\*1)))+(300000\*((40\*50)+(0\*50)+(0\*40)+(45\*70)+(0\*20)))+(100000\*((40\*40)+(0\*20)+(0\*60)+(45\*50)+(0\*10)))+(300000\*((40\*20)+(0\*60)+(0\*50)+(45\*20)+(0\*10)))+(50000\*((4\*30)+(0\*20)+(0\*20)+(45\*30)+(0\*20))))/10000 = **270100**

Risk due to V4 =

((500000\*((5\*4)+(8\*2)+(0\*2)+(6\*3)+(0\*1)))+(300000\*((5\*50)+(8\*40)+(0\*50)+(6\*50)+(0\*10)))+(100000\*((5\*30)+(8\*60)+(0\*60)+(6\*60)+(0\*20)))+(300000\*((5\*20)+(8\*30)+(0\*20)+(6\*40)+(0\*10)))+(5000\*((5\*30)+(8\*60)+(0\*50)+(6\*60)+(0\*30)))+(50000\*((5\*40)+(8\*40)+(0\*30)+(6\*50)+(0\*30))))/10000 = **60695**

Risk due to V5 =

((500000\*((4\*4)+(10\*3)+(6\*2)+(8\*4)+(5\*4)))+(300000\*((4\*40)+(10\*40)+(6\*50)+(8\*60)+(5\*50)))+(100000\*((4\*40)+(10\*40)+(6\*50)+(8\*50)+(5\*40)))+(300000\*((4\*50)+(10\*50)+(6\*60)+(8\*60)+(5\*20)))+(5000\*((4\*40)+(10\*50)+(6\*40)+(8\*50)+(5\*20)))+(50000\*((4\*30)+(10\*30)+(6\*30)+(8\*50)+(5\*30))))/10000 = **123450**

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A12 | 353100 | 1 |
| A2 | 228300 | 2 |
| A10 | 63000 | 3 |
| A14 | 22650 | 4 |
| **A1** | **92700** | **6** |
| A13 | 1195 | 5 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V3 | 270100 | 1 |
| V1 | 174250 | 2 |
| V2 | 127000 | 3 |
| V5 | 123450 | 4 |
| V4 | 60695 | 5 |

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

Applied additional Hardening Controls (for example restricting services or adding a redundant server) to highest ranked Residual Asset Risk, thus further reducing risk impact probabilities, and further reduced the overall security asset residual risk and created a new ranking of vulnerability security risks. In this step we’ve included the value of points from the M-O-T Controls in Step R2 if the value of controls is comparable to value of Critical Assets.

**From R2, the Highest ranked asset is A12 for its risk.** Database of any organization is a central system which stores all the data of it’s working, of it’s planning and of its previous records. This is a major asset and hence the probability of exploiting it is high. This risk can be reduced by installing powerful firewall systems and other security barriers.

Thus, applying the controls on P3 table, the threat-vulnerability pair table with the updated likelihood probabilities will be:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | T7 | Total Threat |
| V1 affects A1, A12 | 30 | 30 | 45 | 40 | 0 | 145 |
| V2 affects A1, A12 | 30 | 30 | 40 | 45 | 0 | 145 |
| V3 affects A1,A2,A10,A12,A14 | 40 | 0 | 0 | 45 | 0 | 85 |
| V4 affects A1,A2,A10,A12,A13,A14 | 5 | 8 | 0 | 6 | 0 | 19 |
| V5 affects A1,A2,A10,A12,A13,A14 | 4 | 10 | 6 | 8 | 5 | 33 |

The probability table of threat exploiting vulnerability will be updated as:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Likelihood of Threat exploiting the vulnerability | | | | | | | | | | | | | | | | | | | | | | | | |
| Asset | T3\*V1 | T3\*V2 | T3\*V3 | T3\*V4 | T3\*V5 | T4\*V1 | T4\*V2 | T4\*V3 | T4\*V4 | T4\*V5 | T5\*V1 | T5\*V2 | T5\*V3 | T5\*V4 | T5\*V5 | T6\*V1 | T6\*V2 | T6\*V3 | T6\*V4 | T6\*V5 | T7\*V1 | T7\*V2 | T7\*V3 | T7\*V4 | T7\*V5 |
| A1 | 3 | 2 | 6 | 4 | 4 | 6 | 3 | 3 | 2 | 3 | 5 | 5 | 3 | 2 | 2 | 5 | 6 | 3 | 3 | 4 | 1 | 2 | 1 | 1 | 4 |
| A2 | 0 | 0 | 50 | 50 | 40 | 0 | 0 | 50 | 40 | 40 | 0 | 0 | 40 | 50 | 50 | 0 | 0 | 70 | 50 | 60 | 0 | 0 | 20 | 10 | 50 |
| A10 | 0 | 0 | 40 | 30 | 40 | 0 | 0 | 20 | 60 | 40 | 0 | 0 | 60 | 60 | 50 | 0 | 0 | 50 | 60 | 50 | 0 | 0 | 10 | 20 | 40 |
| **A12** | **5** | **3** | **2** | **2** | **5** | **2** | **2** | **6** | **3** | **5** | **3** | **2** | **5** | **2** | **6** | **3** | **2** | **2** | **4** | **6** | **2** | **2** | **1** | **1** | **2** |
| A13 | 0 | 0 | 0 | 30 | 40 | 0 | 0 | 0 | 60 | 50 | 0 | 0 | 0 | 50 | 40 | 0 | 0 | 0 | 60 | 50 | 0 | 0 | 0 | 30 | 20 |
| A14 | 0 | 0 | 30 | 30 | 40 | 0 | 0 | 20 | 30 | 40 | 0 | 0 | 20 | 30 | 30 | 0 | 0 | 30 | 50 | 50 | 0 | 0 | 20 | 30 | 30 |

**Calculations for Residual Asset Security Risk**

Asset A1 Risk = (500000\*((30\*3)+(30\*2)+(40\*6)+(5\*4)+(4\*4)+(30\*6)+(30\*3)+(0\*3)+(8\*2)+(10\*3)+(45\*5)+(40\*5)+(0\*3)+(0\*2)+(6\*2)+(40\*5)+(45\*6)+(45\*3)+(6\*3)+(8\*4)+(0\*1)+(0\*2)+(0\*1)+(0\*1)+(5\*4)))/10000 = **92700**

Asset A2 Risk =

(300000\*((40\*50)+(5\*50)+(4\*40)+(0\*50)+(8\*40)+(10\*40)+(0\*40)+(0\*50)+(6\*50)+(45\*70)+(6\*50)+(8\*60)+(0\*20)+(0\*10)+(5\*50)))/ 10000 = **228300**

Asset A10 Risk =

(100000\*((40\*40)+(5\*30)+(4\*40)+(0\*20)+(8\*60)+(10\*40)+(0\*60)+(0\*60)+(6\*50)+(45\*50)+(6\*60)+(8\*50)+(0\*10)+(0\*20)+(5\*40)))/ 10000 = **63000**

**Asset A12 Risk =**

**(300000\*((30\*5)+(30\*3)+(40\*2)+(5\*2)+(4\*5)+(30\*2)+(30\*2)+(0\*6)+(8\*3)+(10\*5)+(45\*3)+(40\*2)+(0\*5)+(0\*2)+(6\*6)+(40\*3)+(45\*2)+(45\*2)+(6\*4)+(8\*6)+(0\*2)+(0\*2)+(0\*1)+(0\*1)+(5\*2)))/10000 = 35310**

Asset A13 Risk =

(5000\*((5\*30)+(4\*40)+(8\*60)+(10\*50)+(0\*50)+(6\*40)+(6\*60)+(8\*50)+(0\*30)+(5\*20)))/ 10000 = **1195**

Asset A14 Risk =

(50000\*((40\*30)+(5\*30)+(4\*40)+(0\*20)+(8\*30)+(10\*40)+(0\*20)+(0\*30)+(6\*30)+(45\*30)+(6\*50)+(8\*50)+(0\*20)+(0\*30)+(5\*30)))/ 10000 =**22650**

**Calculations for Residual Vulnerability Security Risk**

Risk due to V1 = ((500000\*((30\*3)+(30\*6)+(45\*5)+(40\*5)+(0\*1))+(300000\*((30\*5)+(30\*2)+(45\*3)+(40\*3)+(0\*2)))))/10000 = **48700**

Risk due to V2 = ((500000\*((30\*2)+(30\*3)+(40\*5)+(45\*6)+(0\*2)))+(300000\*((30\*3)+(30\*2)+(40\*2)+(45\*2)+(0\*2))))/10000 = **40600**

Risk due to V3 =

((500000\*((40\*6)+(0\*3)+(0\*3)+(45\*3)+(0\*1)))+(300000\*((40\*50)+(0\*50)+(0\*40)+(45\*70)+(0\*20)))+(100000\*((40\*40)+(0\*20)+(0\*60)+(45\*50)+(0\*10)))+(300000\*((40\*2)+(0\*6)+(0\*5)+(45\*2)+(0\*1)))+(50000\*((4\*30)+(0\*20)+(0\*20)+(45\*30)+(0\*20))))/10000 = **224200**

Risk due to V4 =

((500000\*((5\*4)+(8\*2)+(0\*2)+(6\*3)+(0\*1)))+(300000\*((5\*50)+(8\*40)+(0\*50)+(6\*50)+(0\*10)))+(100000\*((5\*30)+(8\*60)+(0\*60)+(6\*60)+(0\*20)))+(300000\*((5\*2)+(8\*3)+(0\*2)+(6\*4)+(0\*1)))+(5000\*((5\*30)+(8\*60)+(0\*50)+(6\*60)+(0\*30)))+(50000\*((5\*40)+(8\*40)+(0\*30)+(6\*50)+(0\*30))))/10000 = **45035**

Risk due to V5 =

((500000\*((4\*4)+(10\*3)+(6\*2)+(8\*4)+(5\*4)))+(300000\*((4\*40)+(10\*40)+(6\*50)+(8\*60)+(5\*50)))+(100000\*((4\*40)+(10\*40)+(6\*50)+(8\*50)+(5\*40)))+(300000\*((4\*5)+(10\*5)+(6\*6)+(8\*6)+(5\*2)))+(5000\*((4\*40)+(10\*50)+(6\*40)+(8\*50)+(5\*20)))+(50000\*((4\*30)+(10\*30)+(6\*30)+(8\*50)+(5\*30))))/10000 = **79170**

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A2 | 228300 | 1 |
| A10 | 63000 | 2 |
| A14 | 22650 | 3 |
| A1 | 92700 | 4 |
| **A12** | **35310** | **5** |
| A13 | 1195 | 6 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V3 | 224200 | 1 |
| V5 | 79170 | 2 |
| V1 | 48700 | 3 |
| V4 | 45035 | 4 |
| V2 | 40600 | 5 |

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

The HGA controls listed were further strengthened by the controls proposed by the CISO and the team. Additionally, MOT(Management-Operational-Technical) controls and VPN plus DMZ controls were added to ensure an overall secure infrastructure. Even after such strong controls have been included in the strategy, a few more could be added and this information could be obtained through the understanding of Common Criteria(CC). CC is a framework that allows employees of organizations who tend to be the users to specify security requirements.

According to CC, the CISO and team could focus on the kind of decisions to be taken considering the risk of using specific IT products and systems in their environments. It further also helps to develop risk mitigation strategies. This information helps in the development and implementation of security risk response strategies.

**Mixed** **Security Risk Prevention Strategy and Security Risk Response (Resilience) Strategy**

**Create a list of all proposed preventions and response security controls. Create a ranking of residual risks for assets and total HGA residual risk, and a ranking for vulnerability risks. Estimate a Risk Prevention budget, a Risk Response budget, and a mixed strategy budget.**

Now, when both Preventive and Responsive strategies are applied together, the probabilities are reduced drastically. The preventive measures include to install new or update old security softwares, verification of data sheets, and access control. The responsive measures could be containing the attack, restricting access and adding stronger security systems(firewalls).

The threat-vulnerability pair table with the reduced likelihood probabilities will be:

|  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- |
|  | T3 | T4 | T5 | T6 | T7 | Total Threat |
| V1 affects A1, A12 | 30 | 30 | 45 | 40 | 0 | 145 |
| V2 affects A1, A12 | 30 | 30 | 40 | 45 | 0 | 145 |
| V3 affects A1,A2,A10,A12,A14 | 40 | 0 | 0 | 45 | 0 | 85 |
| V4 affects A1,A2,A10,A12,A13,A14 | 5 | 8 | 0 | 6 | 0 | 19 |
| V5 affects A1,A2,A10,A12,A13,A14 | 4 | 10 | 6 | 8 | 5 | 33 |

The probability table of threat exploiting vulnerability will be updated as:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | Likelihood of Threat exploiting the vulnerability | | | | | | | | | | | | | | | | | | | | | | | | | |
| Asset | T3\*V1 | T3\*V2 | T3\*V3 | T3\*V4 | T3\*V5 | T4\*V1 | T4\*V2 | T4\*V3 | T4\*V4 | T4\*V5 | T5\*V1 | T5\*V2 | T5\*V3 | T5\*V4 | T5\*V5 | T6\*V1 | T6\*V2 | T6\*V3 | T6\*V4 | T6\*V5 | T7\*V1 | T7\*V2 | T7\*V3 | T7\*V4 | T7\*V5 |
| A1 | 3 | 2 | 6 | 4 | 4 | 6 | 3 | 3 | 2 | 3 | 5 | 5 | 3 | 2 | 2 | 5 | 6 | 3 | 3 | 4 | 1 | 2 | 1 | 1 | 4 |
| A2 | 0 | 0 | 5 | 5 | 4 | 0 | 0 | 5 | 4 | 4 | 0 | 0 | 4 | 5 | 5 | 0 | 0 | 7 | 5 | 6 | 0 | 0 | 2 | 1 | 5 |
| A10 | 0 | 0 | 4 | 3 | 4 | 0 | 0 | 2 | 6 | 4 | 0 | 0 | 6 | 6 | 5 | 0 | 0 | 5 | 6 | 5 | 0 | 0 | 1 | 2 | 4 |
| A12 | 5 | 3 | 2 | 2 | 5 | 2 | 2 | 6 | 3 | 5 | 3 | 2 | 5 | 2 | 6 | 3 | 2 | 2 | 4 | 6 | 2 | 2 | 1 | 1 | 2 |
| A13 | 0 | 0 | 0 | 3 | 4 | 0 | 0 | 0 | 6 | 5 | 0 | 0 | 0 | 5 | 4 | 0 | 0 | 0 | 6 | 5 | 0 | 0 | 0 | 3 | 2 |
| A14 | 0 | 0 | 3 | 3 | 4 | 0 | 0 | 2 | 3 | 4 | 0 | 0 | 2 | 3 | 3 | 0 | 0 | 3 | 5 | 5 | 0 | 0 | 2 | 3 | 3 |

**Calculations for Residual Asset Security Risk**

Asset A1 Risk = (500000\*((30\*3)+(30\*2)+(40\*6)+(5\*4)+(4\*4)+(30\*6)+(30\*3)+(0\*3)+(8\*2)+(10\*3)+(45\*5)+(40\*5)+(0\*3)+(0\*2)+(6\*2)+(40\*5)+(45\*6)+(45\*3)+(6\*3)+(8\*4)+(0\*1)+(0\*2)+(0\*1)+(0\*1)+(5\*4)))/10000 = **92700**

Asset A2 Risk =

(300000\*((40\*5)+(5\*5)+(4\*4)+(0\*5)+(8\*4)+(10\*4)+(0\*4)+(0\*5)+(6\*5)+(45\*7)+(6\*5)+(8\*6)+(0\*2)+(0\*1)+(5\*5)))/ 10000 = **22830**

Asset A10 Risk =

(100000\*((40\*4)+(5\*3)+(4\*4)+(0\*2)+(8\*6)+(10\*4)+(0\*6)+(0\*6)+(6\*5)+(45\*5)+(6\*6)+(8\*5)+(0\*1)+(0\*2)+(5\*4)))/ 10000 = **6300**

Asset A12 Risk =

(300000\*((30\*5)+(30\*3)+(40\*2)+(5\*2)+(4\*5)+(30\*2)+(30\*2)+(0\*6)+(8\*3)+(10\*5)+(45\*3)+(40\*2)+(0\*5)+(0\*2)+(6\*6)+(40\*3)+(45\*2)+(45\*2)+(6\*4)+(8\*6)+(0\*2)+(0\*2)+(0\*1)+(0\*1)+(5\*2)))/10000 = **35310**

Asset A13 Risk =

(5000\*((5\*3)+(4\*4)+(8\*6)+(10\*5)+(0\*5)+(6\*4)+(6\*6)+(8\*5)+(0\*3)+(5\*2)))/ 10000 = **119.5**

Asset A14 Risk =

(50000\*((40\*3)+(5\*3)+(4\*4)+(0\*2)+(8\*3)+(10\*4)+(0\*2)+(0\*3)+(6\*3)+(45\*3)+(6\*5)+(8\*5)+(0\*2)+(0\*3)+(5\*3)))/ 10000 =**2265**

**Calculations for Residual Vulnerability Security Risk**

Risk due to V1 = ((500000\*((30\*3)+(30\*6)+(45\*5)+(40\*5)+(0\*1))+(300000\*((30\*5)+(30\*2)+(45\*3)+(40\*3)+(0\*2)))))/10000 = **48700**

Risk due to V2 = ((500000\*((30\*2)+(30\*3)+(40\*5)+(45\*6)+(0\*2)))+(300000\*((30\*3)+(30\*2)+(40\*2)+(45\*2)+(0\*2))))/10000 = **40600**

Risk due to V3 =

((500000\*((40\*6)+(0\*3)+(0\*3)+(45\*3)+(0\*1)))+(300000\*((40\*5)+(0\*5)+(0\*4)+(45\*7)+(0\*2)))+(100000\*((40\*4)+(0\*2)+(0\*6)+(45\*5)+(0\*1)))+(300000\*((40\*2)+(0\*6)+(0\*5)+(45\*2)+(0\*1)))+(50000\*((4\*3)+(0\*2)+(0\*2)+(45\*3)+(0\*2))))/10000 = **43885**

Risk due to V4 =

((500000\*((5\*4)+(8\*2)+(0\*2)+(6\*3)+(0\*1)))+(300000\*((5\*5)+(8\*4)+(0\*5)+(6\*5)+(0\*1)))+(100000\*((5\*3)+(8\*6)+(0\*6)+(6\*6)+(0\*2)))+(300000\*((5\*2)+(8\*3)+(0\*2)+(6\*4)+(0\*1)))+(5000\*((5\*3)+(8\*6)+(0\*5)+(6\*6)+(0\*3)))+(50000\*((5\*4)+(8\*4)+(0\*3)+(6\*5)+(0\*3))))/10000 = **8499.5**

Risk due to V5 =

((500000\*((4\*4)+(10\*3)+(6\*2)+(8\*4)+(5\*4)))+(300000\*((4\*4)+(10\*4)+(6\*5)+(8\*6)+(5\*5)))+(100000\*((4\*4)+(10\*4)+(6\*5)+(8\*5)+(5\*4)))+(300000\*((4\*5)+(10\*5)+(6\*6)+(8\*6)+(5\*2)))+(5000\*((4\*4)+(10\*5)+(6\*4)+(8\*5)+(5\*2)))+(50000\*((4\*3)+(10\*3)+(6\*3)+(8\*5)+(5\*3))))/10000 = **17295**

**Ranking Table of Security Asset Residual Risk**

|  |  |  |
| --- | --- | --- |
| Asset number | Residual Asset Security Risk | RANK |
| A1 | 92700 | 1 |
| A12 | 35310 | 2 |
| A2 | 22830 | 3 |
| A10 | 6300 | 4 |
| A14 | 2265 | 5 |
| A13 | 119.5 | 6 |

**Ranking Table of Vulnerability Security Risk**

|  |  |  |
| --- | --- | --- |
| Vulnerability number | Vulnerability Security Risk | RANK |
| V1 | 48700 | 1 |
| V3 | 43885 | 2 |
| V2 | 40600 | 3 |
| V5 | 17295 | 4 |
| V4 | 8499.5 | 5 |

**Cost Benefit Analysis**

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

The Risk Assessment for HGA is a process of identifying the organization’s assets, probable threats and the vulnerabilities. Additionally, the HGA also has current and new control policies and strategies that help to control and minimize the effect of the threats on the assets. Firstly, after obtaining the set of assets, threats and vulnerabilities, a set of 6 assets, 5 threats and 5 vulnerabilities are chosen and the current HGA security controls are applied to calculate Residual Asset Security Risks and Vulnerability Security Risks. Next, the CISO proposed new security controls are applied and again the Residual Asset Security Risks and Vulnerability Security Risks are calculated and are ranked. In the Security Risk Preventive Strategy, both these current and new security controls are applied together as 3 levels: P1, P2 and P3. P2 where the highest ranked vulnerability in P1 is mitigated and P3 where the highest ranked vulnerability in P2 is mitigated.

For the Security Risk Responsive Strategy, both the current and new security controls are applied together again as 3 levels: R1, R2 and R3. Residual Risk Rankings and Vulnerability Risk Rankings are calculated due to reducing risk impacts to less than 100% based on to implementing M-O-T controls which reduce risk impacts, without though negatively impacting operational effectiveness. R2 is where the highest ranked Asset for its risk in R1 is mitigated and R2 is where the highest ranked Asset for its risk in R2 is mitigated.

Most of the Security controls have been implemented in current and new CISO proposed rules, a few of the missing ones are in the table below. These current, new security controls and MOT controls altogether help in reducing the probabilities of impact to major extent.

|  |  |  |
| --- | --- | --- |
| Management | Operational | Technical |
| Program Management | Incident Reporting and Handling | Audit Trails |
| Risk Management | Security considerations in support and operations |  |
| Life Cycle Planning | Physical and Environmental Security |  |
| Assurance |  |  |

The HGA controls listed were further strengthened by the controls proposed by the CISO and the team. Additionally, MOT(Management-Operational-Technical) controls and VPN plus DMZ controls were added to ensure an overall secure infrastructure. Even after such strong controls have been included in the strategy, a few more could be added and this information could be obtained through the understanding of Common Criteria (CC). CC is a framework that allows employees of organizations who tend to be the users to specify security requirements.

According to CC, the CISO and team could focus on classification of devices and accordingly make “Protection Profiles” which are documents stating security policies for that particular set of devices. It could also ensure the validity of the compliance audits through establishment of the Evaluation Assurance Level (EAL), which is a rating standard that describes the depth and correctness of the evaluation.

According to CC, the CISO and team could also focus on the kind of decisions to be taken considering the risk of using specific IT products and systems in their environments. It further also helps to develop risk mitigation strategies. This information helps in the development and implementation of security risk response strategies.

On a whole, the HGA team addressed most of the security risks. However, stronger security policies as we study in Common Criteria could be used to thus ensure greater assurance of security to the organization’s assets. Measures like Multi-Factor Authentication, having Incident Response Plans, Security Awareness Trainings and conducting regular and genuine Audits. It is therefore important for the organizations to understand that security is an ongoing process and requires ongoing attention and investment to be effective.

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

On comparison of Ranking tables of Security Asset Residual Risk and Vulnerability Security Risk in Scenario 3 for cases P1,P2,P3 and R1,R2,R3 and the mixed strategy tables, it is clearly evident that implementing only preventive or only responsive strategies are not really effective. This could be due to the fact that preventive measures could be heavy security models and are not cost-effective all the time. And not always is the requirement of the responsive measures, they would come into action only when there is an attack.

But, the risks would be the least when both Preventive and Response strategies would be applied together (as seen in the results of mixed strategies) and thus the organization would be efficient and secure. A balanced approach of preventive and response strategies is the key.

**Risk Prevention, Response and Mixed Strategy Budget**

|  |  |  |  |
| --- | --- | --- | --- |
| **Controls** | **Risk Prevention Budget ($)** | **Risk Response Budget ($)** | **Mixed Strategy Budget ($)** |
| Payroll Frauds | 30000 | 20000 | 35000 |
| Payroll Errors | 50000 | 30000 | 60000 |
| Continuation of Operations | 80000 | 70000 | 95000 |
| Protection of data | 100000 | 80000 | 150000 |
| Strong Encryption and Authentication controls | 130000 | 90000 | 145000 |
| Disclosure of sensitive information | 70000 | 30000 | 90000 |
| Virtual Private Network | 20000 | 10000 | 45000 |
| Demilitarized Zone | 40000 | 10000 | 60000 |
| **Total** | **520000** | **340000** | **680000** |

Residual Risk = Risk with Current controls – Risk with New controls

Risk with Current controls = Risk of Assets after considering Current Security Controls

Risk with New controls = Risk of Assets after adding the New controls to the Current Controls

Therefore, Residual Risk = $1255000 – $159524.5

= $1095475.5

**What is the (expected overall security risk reduction Benefit) / (proposed overall security risk budget Cost) ratio for the 3 budgets in XIII?**

Proposed Security Budget cost for the three Budgets:

* Cost Benefit Ratio Analysis for Risk Prevention Budget

= Expected Security Risk Benefit / Proposed Security Risk Prevention Budget Cost

= 1095475.5/520000= 2.1066

* Cost Benefit Ratio Analysis for Risk Response Budget

= Expected Security Risk Benefit / Proposed Security Risk Prevention Budget Cost

= 1095475.5/340000= 3.2219

* Cost Benefit Ratio Analysis for Mixed Strategy Budget ss

= Expected Security Risk Benefit / Proposed Security Mixed Strategy Budget Cost

= 1095475.5/680000= 1.61099

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

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

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

|  |
| --- |
| **Identification Credentials** |
| ID Cards |
| Fingerprint |
| Passwords and security questions |
| Badge readers |
| Security cameras |
| **Personal Authentication** |
| Passwords |
| Biometrics |
| Tokens |
| Mobile authentications |
| Smart cards |
| Security questions |
| **Authorization** |
| Role-based access control (RBAC) |
| Multi-factor authentication (MFA) |
| Access Control List |
| Identity and Access Management (IAM) Policies |
| **Logical Access Control Methods** |
| Digital certificates and PKI |
| Access Control List |
| Pins and Passwords |
| Encryptions and keys |
| Security Information and Event Management (SIEM) |
| VPN |
| Network segmentation |
| Time-based access control |
| Device management |
| Session management |
| **Physical Access Control Methods** |
| Security personnel |
| Security cameras |
| Motion sensors |
| Access cards |
| Proximity sensors |
| Physical barriers |
| Security fences |
| **Biometric Systems** |
| Fingerprint recognition |
| Iris recognition |
| Facial recognition |
| Voice recognition |

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

|  |
| --- |
| **Enclave Protection** |
| Defense in depth |
| Firewalls |
| Network Segmentation |
| VPN |
| DMZ |
| Encryption |
| Routers |
| Intrusion Detection and Prevention Systems (IDS/IPS) |
| Network Test Access Points(TAP) |
| Wireless IDS (WIDS) |
| IPSec VPN Tunnels |
| **Firewalls Risk Management** |
| Packet Filter Firewall |
| Bastion Host |
| Stateful Inspection Firewalls |
| Deep Packet Inspection |
| Application-Proxy Gateway Firewalls |
| Hybrid Technology Firewalls |
| Proxy Servers |
| **Routers Risk Management** |
| Route Table Integrity |
| Securing Router Planes |

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

|  |
| --- |
| **Ports, Protocols and Services (PPS) Risk Management** |
| Three levels of Blocking Protocols |
| Restricting ICMP Echo Requests |
| Restricting Traceroute |
| IPV4 Address Filtering |
| IPV6 Address Filtering |
| Unicast Reverse Path Forwarding |
| SYN Flood attack protecting Servers and LANs |
| SYN Flood attack protecting Routers |
| **Device Risk Management** |
| Vulnerability Management System (VMS) |
| Out-of-Band Management |
| In-Band Management |
| **Device Monitoring, Network Management Risk Management** |
| Simple Network Management Protocol (SNMP) |
| Network Management Station |
| **Network Authentication, Authorization and Accounting Risk Management** |
| Authentication |
| Authorization |
| Accounting |
| Auditing |
| Router Password Protection |
| **Network Intrusion Detection Risk Management** |
| Local Area NIDS |
| External NIDS |
| **Switches and VLAN’s Risk Management** |
| Physical |
| Virtual Local Area Networks (VLAN’s) |
| VLAN Trunking |
| VLAN Access and Port Authentication |
| VLAN 802.1X and Management Policy Server |
| **Virtual Private Network Risk Management** |
| Gateway-to-Gateway |
| Host-to-gateway |
| Host-to-host |

1. **Database Security Risk Management Implementation Controls and Policies**

|  |
| --- |
| **Authentication – User Accounts** |
| Application User |
| Database Administrator (DBA) |
| Application Owner |
| Application User Manager |
| Application Account |
| Database Auditor |
| Database Operator |
| Password policies |
| Regularly review and update access controls |
| **Authorization** |
| Role Based Access Control (RBAC) |
| Multi-tier Applications |
| Policies to define access levels |
| **Confidentiality** |
| Encryption of data in database |
| Encryption of Application code |
| Protection of data files |
| Training |
| **Data Integrity** |
| Transaction Logging and journaling |
| Database capabilities |
| Version Control |
| **Auditing** |
| Deciding on auditing connections |
| Auditing privileged activities |
| Auditing of changes to data |
| Automated tools |
| Automated reporting capability |
| **Replication and Federation** |
| Database Replication |
| Federated database |
| **Clustering** |
| Database clustering |
| **Backup and Recovery** |
| Database backup and recovery |
| **OS Protections** |
| Disk Partitions |
| Having dedicated OS accounts |
| Component separation of directories and files |
| DBA |
| Implement patch management |
| Monitor System Logs |
| **Application Protections** |
| Review of Authentication method |
| Application protections |
| **Network Protections** |
| Intrusion Detection and Prevention systems (IDS/IPS) |
| Virtual private networks (VPNs) |
| Implementing network segmentation |
| **Security Design and Configuration** |
| Procedural Review |
| Configuration Specifications |
| Compliance Testing |
| Non-Repudiation |
| System Library Management Controls |
| Security Support Structure Partitioning |
| System State Changes |
| Software Baseline |
| **Enclave and Computing Environment** |
| Audit Trail, Monitoring, Analysis and Reporting |
| Security Monitoring |
| Physical Security |
| Incident Response Plan |
| **Business Continuity** |
| Protection of Backup and Restoration Assets |
| Disaster and Recovery Planning |
| Backup copies of Critical Software |
| **Vulnerability and Incident Management** |
| Vulnerability Scanning |
| Incident Response Plan |
| Incident Response Team |

1. **Applications Development Security Risk Management Implementation Controls and Policy**

|  |
| --- |
| **Application Data Handling** |
| Database Management System (DBMS) |
| Data storage |
| In-Memory Data Handling |
| Data Transmission |
| Data Integrity |
| Data Marking |
| **Authentication** |
| Server Authentication |
| User Authentication |
| Single Code Identification |
| **Use of Cryptography** |
| Ciphers |
| Message Authentication Codes |
| Encryption for data at rest |
| Authentication protocol |
| **User Accounts** |
| Time Period and Lockouts |
| Access control |
| Duplicate accounts |
| **Input Validation** |
| Criteria check |
| Implementing controls to manage SQL Injection vulnerabilities |
| Manage Integer overflows |
| Managing format String Vulnerabilities |
| Managing canonical Representation issues |
| Command Injection Vulnerabilities |
| Managing buffer overflows |
| **Auditing** |
| Recorded Login information |
| **Configuration Management** |
| Software Configuration Management |
| **Testing** |
| Reviewing policies |
| Identifying testing criteria |
| Conducting tests |
| Analyzing results |
| Web Application Vulnerability Scanners |
| **Deployment** |
| System Security Plan |
| Data Classification Guide |
| Threat Model |
| Application Configuration Guide |
| Third Party Software Guide |
| Ports and Protocols Guide |
| Workplace Security Procedures |

1. **Wireless Security Risk Management Implementation Controls and Policies**

|  |
| --- |
| **Wireless LAN Risk Management** |
| Extensible Authentication Protocol (EAP) |
| EAP Transport Layer Security |
| EAP Tunneling transport layer Security |
| Protected Extensible Authentication Protocol (PEAP) |
| Lightweight Extensible Authentication Protocol (LEAP) |
| Separation of wireless and wired network |
| Communication channels of LAN |
| Usage of different standards |
| WEP, WPA protocol |
| Security Tunnels |
| Service Set Identifier (SSID) |
| MAC addresses |
| DOD requirements |
| **Wireless PAN Risk Management** |
| IEEE 802.15 WPAN standard |
| PIN/ Legacy pairing |
| **Wireless WAN Risk Management** |
| CDPD |
| IEEE 802.16 BWA |
| **Wireless RFID Risk Management** |
| Encryption |
| Use of Secure Protocols |
| Use of Anti-Collision Algorithms |
| **Wireless PED Risk Management** |
| Smart Card Security |
| NSA Type 1 certification |

1. **For 1-6 Tables above:**

**List of Cybersecurity Implementation Controls present at Larsen & Toubro Infotech – LTI**

|  |
| --- |
| **Identification Credentials** |
| ID Cards |
| Fingerprint |
| Passwords and security questions |
| Security cameras |
| **Personal Authentication** |
| Passwords |
| Biometrics |
| Tokens |
| Mobile authentications |
| Smart cards |
| Security questions |
| **Authorization** |
| Role-based access control (RBAC) |
| Multi-factor authentication (MFA) |
| Access Control List |
| Identity and Access Management (IAM) Policies |
| **Logical Access Control Methods** |
| Digital certificates and PKI |
| Access Control List |
| Pins and Passwords |
| Encryptions and keys |
| Security Information and Event Management (SIEM) |
| VPN |
| Network segmentation |
| Time-based access control |
| Device management |
| Session management |
| **Physical Access Control Methods** |
| Security personnel |
| Security cameras |
| Motion sensors |
| Access cards |
| Physical barriers |
| Security fences |
| **Biometric Systems** |
| Fingerprint recognition |
| **Enclave Protection** |
| Defense in depth |
| Firewalls |
| Network Segmentation |
| Encryption |
| Routers |
| Intrusion Detection and Prevention Systems (IDS/IPS) |
| Network Test Access Points(TAP) |
| IPSec VPN Tunnels |
| **Firewalls Risk Management** |
| Packet Filter Firewall |
| Stateful Inspection Firewalls |
| Deep Packet Inspection |
| Application-Proxy Gateway Firewalls |
| **Routers Risk Management** |
| Securing Router Planes |
| **Ports, Protocols and Services (PPS) Risk Management** |
| Three levels of Blocking Protocols |
| Restricting ICMP Echo Requests |
| Restricting Traceroute |
| IPV4 Address Filtering |
| IPV6 Address Filtering |
| Unicast Reverse Path Forwarding |
| **Device Risk Management** |
| Vulnerability Management System (VMS) |
| In-Band Management |
| **Device Monitoring, Network Management Risk Management** |
| Simple Network Management Protocol (SNMP) |
| Network Management Station |
| **Network Authentication, Authorization and Accounting Risk Management** |
| Authentication |
| Authorization |
| Accounting |
| Auditing |
| Router Password Protection |
| **Network Intrusion Detection Risk Management** |
| Local Area NIDS |
| External NIDS |
| **Switches and VLAN’s Risk Management** |
| Physical |
| Virtual Local Area Networks (VLAN’s) |
| VLAN Trunking |
| **Virtual Private Network Risk Management** |
| Gateway-to-Gateway |
| Host-to-gateway |
| Host-to-host |
| **Authentication – User Accounts** |
| Application User |
| Database Administrator (DBA) |
| Application Owner |
| Application User Manager |
| Application Account |
| Database Auditor |
| Password policies |
| **Authorization** |
| Role Based Access Control (RBAC) |
| Multi-tier Applications |
| **Confidentiality** |
| Encryption of data in database |
| Training |
| **Data Integrity** |
| Transaction Logging and journaling |
| Database capabilities |
| Version Control |
| **Auditing** |
| Deciding on auditing connections |
| Auditing privileged activities |
| Auditing of changes to data |
| **Replication and Federation** |
| Database Replication |
| Federated database |
| **Clustering** |
| Database clustering |
| **Backup and Recovery** |
| Database backup and recovery |
| **OS Protections** |
| Disk Partitions |
| Having dedicated OS accounts |
| Component separation of directories and files |
| Implement patch management |
| Monitor System Logs |
| **Application Protections** |
| Review of Authentication method |
| Application protections |
| **Network Protections** |
| Intrusion Detection and Prevention systems (IDS/IPS) |
| Virtual private networks (VPNs) |
| Implementing network segmentation |
| **Security Design and Configuration** |
| Procedural Review |
| Configuration Specifications |
| Compliance Testing |
| Non-Repudiation |
| System Library Management Controls |
| Security Support Structure Partitioning |
| **Enclave and Computing Environment** |
| Audit Trail, Monitoring, Analysis and Reporting |
| Security Monitoring |
| Physical Security |
| Incident Response Plan |
| **Business Continuity** |
| Protection of Backup and Restoration Assets |
| Disaster and Recovery Planning |
| Backup copies of Critical Software |
| **Vulnerability and Incident Management** |
| Vulnerability Scanning |
| Incident Response Plan |
| Incident Response Team |
| **Application Data Handling** |
| Database Management System (DBMS) |
| Data storage |
| In-Memory Data Handling |
| Data Transmission |
| Data Integrity |
| **Authentication** |
| Server Authentication |
| User Authentication |
| **Use of Cryptography** |
| Ciphers |
| Message Authentication Codes |
| Authentication protocol |
| **User Accounts** |
| Access control |
| Duplicate accounts |
| **Input Validation** |
| Criteria check |
| Implementing controls to manage SQL Injection vulnerabilities |
| Manage Integer overflows |
| Managing format String Vulnerabilities |
| Managing canonical Representation issues |
| **Auditing** |
| Recorded Login information |
| **Configuration Management** |
| Software Configuration Management |
| **Testing** |
| Reviewing policies |
| Identifying testing criteria |
| Conducting tests |
| Analyzing results |
| Web Application Vulnerability Scanners |
| **Deployment** |
| System Security Plan |
| Data Classification Guide |
| Threat Model |
| Application Configuration Guide |
| Third Party Software Guide |
| Ports and Protocols Guide |
| Workplace Security Procedures |
| **Wireless LAN Risk Management** |
| Extensible Authentication Protocol (EAP) |
| EAP Transport Layer Security |
| Protected Extensible Authentication Protocol (PEAP) |
| Lightweight Extensible Authentication Protocol (LEAP) |
| Separation of wireless and wired network |
| Communication channels of LAN |
| Usage of different standards |
| Security Tunnels |
| MAC addresses |
| DOD requirements |
| **Wireless PAN Risk Management** |
| IEEE 802.15 WPAN standard |
| PIN/ Legacy pairing |
| **Wireless WAN Risk Management** |
| CDPD |
| IEEE 802.16 BWA |
| **Wireless RFID Risk Management** |
| Encryption |
| Use of Secure Protocols |
| **Wireless PED Risk Management** |
| Smart Card Security |
| NSA Type 1 certification |

**Comparison of the Implementation controls discussed with Larsen and Toubro - LTI’s existing Cybersecurity Implementation controls**

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

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Controls** |
| **Identification Credentials** |  |
| ID Cards | Present |
| Fingerprint | Present |
| Passwords and security questions | Present |
| Badge readers | Absent |
| Security cameras | Present |
| **Personal Authentication** |  |
| Passwords | Present |
| Biometrics | Partial |
| Tokens | Present |
| Mobile authentications | Present |
| Smart cards | Present |
| Security questions | Present |
| **Authorization** |  |
| Role-based access control (RBAC) | Present |
| Multi-factor authentication (MFA) | Present |
| Access Control List | Present |
| Identity and Access Management (IAM) Policies | Present |
| **Logical Access Control Methods** |  |
| Digital certificates and PKI | Present |
| Access Control List | Present |
| Pins and Passwords | Present |
| Encryptions and keys | Present |
| Security Information and Event Management (SIEM) | Present |
| VPN | Present |
| Network segmentation | Present |
| Time-based access control | Partial |
| Device management | Present |
| Session management | Present |
| **Physical Access Control Methods** |  |
| Security personnel | Present |
| Security cameras | Present |
| Motion sensors | Present |
| Access cards | Present |
| Proximity sensors | Absent |
| Physical barriers | Present |
| Security fences | Present |
| **Biometric Systems** |  |
| Fingerprint recognition | Present |
| Iris recognition | Absent |
| Facial recognition | Absent |
| Voice recognition | Absent |

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

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Controls** |
| **Enclave Protection** |  |
| Defense in depth | Present |
| Firewalls | Present |
| Network Segmentation | Present |
| VPN | Absent |
| DMZ | Absent |
| Encryption | Present |
| Routers | Present |
| Intrusion Detection and Prevention Systems (IDS/IPS) | Present |
| Network Test Access Points(TAP) | Present |
| Wireless IDS (WIDS) | Absent |
| IPSec VPN Tunnels | Present |
| **Firewalls Risk Management** |  |
| Packet Filter Firewall | Present |
| Bastion Host | Absent |
| Stateful Inspection Firewalls | Present |
| Deep Packet Inspection | Present |
| Application-Proxy Gateway Firewalls | Present |
| Hybrid Technology Firewalls | Absent |
| Proxy Servers | Absent |
| **Routers Risk Management** |  |
| Route Table Integrity | Absent |
| Securing Router Planes | Present |

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

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Controls** |
| **Ports, Protocols and Services (PPS) Risk Management** |  |
| Three levels of Blocking Protocols | Present |
| Restricting ICMP Echo Requests | Present |
| Restricting Traceroute | Present |
| IPV4 Address Filtering | Present |
| IPV6 Address Filtering | Present |
| Unicast Reverse Path Forwarding | Present |
| SYN Flood attack protecting Servers and LANs | Absent |
| SYN Flood attack protecting Routers | Absent |
| **Device Risk Management** |  |
| Vulnerability Management System (VMS) | Present |
| Out-of-Band Management | Absent |
| In-Band Management | Present |
| **Device Monitoring, Network Management Risk Management** |  |
| Simple Network Management Protocol (SNMP) | Present |
| Network Management Station | Present |
| **Network Authentication, Authorization and Accounting Risk Management** |  |
| Authentication | Present |
| Authorization | Present |
| Accounting | Present |
| Auditing | Present |
| Router Password Protection | Present |
| **Network Intrusion Detection Risk Management** |  |
| Local Area NIDS | Present |
| External NIDS | Present |
| **Switches and VLAN’s Risk Management** |  |
| Physical | Present |
| Virtual Local Area Networks (VLAN’s) | Present |
| VLAN Trunking | Present |
| VLAN Access and Port Authentication | Absent |
| VLAN 802.1X and Management Policy Server | Absent |
| **Virtual Private Network Risk Management** |  |
| Gateway-to-Gateway | Present |
| Host-to-gateway | Present |
| Host-to-host | Present |

1. **Database Security Risk Management Implementation Controls and Policies**

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Controls** |
| **Authentication – User Accounts** |  |
| Application User | Present |
| Database Administrator (DBA) | Present |
| Application Owner | Present |
| Application User Manager | Present |
| Application Account | Present |
| Database Auditor | Present |
| Database Operator | Absent |
| Password policies | Present |
| Regularly review and update access controls | Absent |
| **Authorization** |  |
| Role Based Access Control (RBAC) | Present |
| Multi-tier Applications | Present |
| Policies to define access levels | Absent |
| **Confidentiality** |  |
| Encryption of data in database | Present |
| Encryption of Application code | Absent |
| Protection of data files | Absent |
| Training | Present |
| **Data Integrity** |  |
| Transaction Logging and journaling | Present |
| Database capabilities | Present |
| Version Control | Present |
| **Auditing** |  |
| Deciding on auditing connections | Present |
| Auditing privileged activities | Present |
| Auditing of changes to data | Present |
| Automated tools | Absent |
| Automated reporting capability | Absent |
| **Replication and Federation** |  |
| Database Replication | Present |
| Federated database | Present |
| **Clustering** |  |
| Database clustering | Present |
| **Backup and Recovery** |  |
| Database backup and recovery | Present |
| **OS Protections** |  |
| Disk Partitions | Present |
| Having dedicated OS accounts | Present |
| Component separation of directories and files | Present |
| DBA | Absent |
| Implement patch management | Present |
| Monitor System Logs | Present |
| **Application Protections** |  |
| Review of Authentication method | Present |
| Application protections | Present |
| **Network Protections** |  |
| Intrusion Detection and Prevention systems (IDS/IPS) | Present |
| Virtual private networks (VPNs) | Present |
| Implementing network segmentation | Present |
| **Security Design and Configuration** |  |
| Procedural Review | Present |
| Configuration Specifications | Present |
| Compliance Testing | Present |
| Non-Repudiation | Present |
| System Library Management Controls | Present |
| Security Support Structure Partitioning | Present |
| System State Changes | Absent |
| Software Baseline | Absent |
| **Enclave and Computing Environment** |  |
| Audit Trail, Monitoring, Analysis and Reporting | Present |
| Security Monitoring | Present |
| Physical Security | Present |
| Incident Response Plan | Present |
| **Business Continuity** |  |
| Protection of Backup and Restoration Assets | Present |
| Disaster and Recovery Planning | Present |
| Backup copies of Critical Software | Present |
| **Vulnerability and Incident Management** |  |
| Vulnerability Scanning | Present |
| Incident Response Plan | Present |
| Incident Response Team | Present |

1. **Applications Development Security Risk Management Implementation Controls and Policy**

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Controls** |
| **Application Data Handling** |  |
| Database Management System (DBMS) | 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 |
| Single Code Identification | Absent |
| **Use of Cryptography** |  |
| Ciphers | Present |
| Message Authentication Codes | Present |
| Encryption for data at rest | Absent |
| Authentication protocol | Present |
| **User Accounts** |  |
| Time Period and Lockouts | Absent |
| Access control | Present |
| Duplicate accounts | Present |
| **Input Validation** |  |
| Criteria check | Present |
| Implementing controls to manage SQL Injection vulnerabilities | Present |
| Manage Integer overflows | Present |
| Managing format String Vulnerabilities | Present |
| Managing canonical Representation issues | Present |
| Command Injection Vulnerabilities | Absent |
| Managing buffer overflows | Absent |
| **Auditing** |  |
| Recorded Login information | Present |
| **Configuration Management** |  |
| Software Configuration Management | Present |
| **Testing** |  |
| Reviewing policies | Present |
| Identifying testing criteria | Present |
| Conducting tests | Present |
| Analyzing results | Present |
| Web Application Vulnerability Scanners | Present |
| **Deployment** |  |
| System Security Plan | Present |
| Data Classification Guide | Present |
| Threat Model | Present |
| Application Configuration Guide | Present |
| Third Party Software Guide | Present |
| Ports and Protocols Guide | Present |
| Workplace Security Procedures | Present |

1. **Wireless Security Risk Management Implementation Controls and Policies**

|  |  |
| --- | --- |
| **Cybersecurity Implementation Controls** | **Implementation Controls** |
| **Wireless LAN Risk Management** |  |
| Extensible Authentication Protocol (EAP) | Present |
| EAP Transport Layer Security | Present |
| EAP Tunneling transport layer Security | Absent |
| Protected Extensible Authentication Protocol (PEAP) | Present |
| Lightweight Extensible Authentication Protocol (LEAP) | Present |
| Separation of wireless and wired network | Present |
| Communication channels of LAN | Present |
| Usage of different standards | Present |
| WEP, WPA protocol | Absent |
| Security Tunnels | Present |
| Service Set Identifier (SSID) | Absent |
| MAC addresses | Present |
| DOD requirements | Present |
| **Wireless PAN Risk Management** |  |
| IEEE 802.15 WPAN standard | Present |
| PIN/ Legacy pairing | Partial |
| **Wireless WAN Risk Management** |  |
| CDPD | Present |
| IEEE 802.16 BWA | Present |
| **Wireless RFID Risk Management** |  |
| Encryption | Present |
| Use of Secure Protocols | Present |
| Use of Anti-Collision Algorithms | Absent |
| **Wireless PED Risk Management** |  |
| Smart Card Security | Present |
| NSA Type 1 certification | Present |

**List of Critical Assets in $ that exist in Larsen & Toubro Infotech – LTI**

|  |  |  |
| --- | --- | --- |
| **Asset Number** | **Asset Name** | **Asset Value** |
| A1 | Financial resources | $500000 |
| A2 | Network Devices (PC’s, Modems, Routers, Printers and other such Relay points) | $1000000 |
| A3 | Database and other Storage devices | $700000 |
| A4 | Security systems (firewalls and encryption systems) | $400000 |
| A5 | Personnel information and documents of information | $300000 |
| A6 | Reputation | Intangible |

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

1. Manual checking
2. Ease of unauthorized access
3. Ease of fooling the systems
4. Sensitive information disclosure
5. Social Engineering
6. Increase Attack surface
7. Increase in Cyber attacks
8. Data interception
9. Unknown data modifications/stealing of data
10. Difficulty in monitoring user activity
11. SYN Attacks flooding
12. Interruption in operations
13. Lack of system security
14. Ease of VLAN access
15. Lack of port security
16. No Privilege controls
17. Security breach
18. Compliance violation
19. Reduced efficiency
20. Inconsistent access control
21. Higher risk of errors
22. Unknown data/file modifications
23. Limited traceability
24. Difficulty in prioritizing important assets
25. Difficulty in establishing data privacy laws and policies
26. Difficulty in implementing software testing processes
27. Lower rate of performance
28. Malware infection
29. System crashes
30. Increased Man-in-the-middle attacks
31. Identity spoofing
32. Denial of Service attacks
33. Difficulty in identifying networks
34. Interference with other networks
35. Compatibility issues
36. User experience issues
37. Increased rate of Collisions
38. Reduced accuracy

**List of potential threats to your company that could exploit vulnerabilities of critical assets**

1. Confidentiality and Privacy issues
2. Integrity issues
3. Availability issues
4. Authentication issues
5. Non-Repudiation issues
6. Access Control issues
7. Loss or Harm to Assets

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

1. Disclosure of organizational data
2. Manipulations to data
3. Increase in attack probabilities
4. Lack of compliance
5. Operational failures
6. Unauthorized access
7. Loss of data and privacy
8. Pose danger to the survival of the organization
9. Increased attack area
10. Losing access control
11. Costs and Efficiency
12. Exploit the organizational networks and devices
13. Fraudulent and unknown modifications to data and networks
14. Network Congestion
15. Resource depletion
16. Reduced productivity
17. Privacy and Compliance violation
18. Business disruption
19. Data breach
20. Insider Threat
21. Loss of reputation
22. Increased vulnerabilities to assets
23. Effects to rate/efficiency of production
24. Higher risk of error
25. Compromise the sensitive information
26. Risk of being less compliant to industry-specific regulations and data privacy laws
27. Higher likelihood of software bugs and errors
28. Increased brute force attacks
29. Increased denial of service attacks
30. Database attacks
31. Increase in malware attacks
32. Fraudulent activity
33. Network downtime
34. Reputation damage
35. Network congestion

**List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks (it is not required to write detailed policies) – Risk Prevention Strategy**

1. The problem of time delays and inefficiencies due to manual user verifications which pave path for easy unauthorized access can be solved by installing automatic badge detecting systems or scanners.
2. The biometric systems could use multiple verification and security measures instead of a single one. The finger readers could be parallely connected to facial and iris scanners. This integration of various methods would only strengthen the security of the organization more to a greater extent.
3. There needs to be log out periods for all organizational devices on a daily basis. This needs to be implemented to decrease the risk of unauthorized access.
4. Proximity sensors that detect access cards near to them need to be installed in secure areas. These sensors work to cancel access when these cards are no longer nearby to them. This can be the most secure way to protect extremely secure and private areas
5. Iris recognitions which are considered to be the most secure and strongest biometric checks need to be implemented in the organization as these iris readers cannot be fooled as easily as finger scanners are fooled.
6. Facial and Voice recognition systems need to be implemented for virtual communication security. These systems help to verify the remote user and thus ensure security.
7. It is always a good practice to maintain at least 3 copies of the whole organizational data at various distant databases at different places. Independency of backups helps to mitigate and re-obtain original data in case of unauthorized access and manipulated data. Incremental backup is the best option of all.
8. Unauthorized access which accounts to be the most serious problem can be solved by hardening the access controls and the verification systems. Instead of having a single verification systems like finger print reader, additionally we can integrate this system to a parallel verification system like Multi factor authentication (MFA) or One Time Password (OTP) systems.
9. Loss of data due unauthorized access can be serious, it is advised for companies to store atleast 3 copies of the whole organizational data into different databases at different locations of the world. This might help to recover data in case of data deletion and loss.
10. The attack area can be decreased by sub-networking. All departments of the organization need to work independent of one another such that even if one department is down, all others are functional and are not affected by the failure of the other networks.
11. There might be numerous options for security controls in the market. It is important to choose the most effective one, the one which provides the numerous services and finally the cost factor is also to be considered.
12. Network Congestions issues can be prevented using an increased bandwidth for the networks or also to install filters that prioritize authorized access requests.
13. Load-balancers could be utilized to the fullest in cases of high network congestion to not overuse one device/server and cause failure.
14. Loss of data due unauthorized access can be serious; it is advised for companies to store at least 3 copies of the whole organizational data into different databases at different locations of the world. This might help to recover data in case of data deletion and loss.
15. There might be numerous options for security controls in the market. It is important to choose the most effective one, the one which provides the numerous services and finally the cost factor is also to be considered.
16. Regularly review access controls and permissions to ensure that only authorized users and devices have access to the network and VLANs.
17. Use an RBAC system to define user roles and access permissions based on their job requirements. This ensures that users only have access to the resources they need to do their jobs.
18. Stronger firewalls implementation to scan the packets of their origin, their intent and their destination is crucial.
19. Stronger anti-virus, anti-malware software is required to be implemented on all the user devices to prevent any kind of virus/worm/malware or any other malicious harm causing software
20. Identity and Access Management (IAM) policies are to be prepared by the root user (the administrator) so that this policy is used to manage access controls among the leaf users.
21. Centralized Syslog Servers need to be installed. These servers are a kind that help to tabulate all intrusion data, data fields are: Time of intrusion, Hostname (default gateway), and Message (which has IP signature and Risk rating data)​
22. Assign a Data Operator to manage all privilege controls. A separate role in order to maintain, analyze and control the access to any user is crucial. Data operators can help identify patterns and trends within a company's user controls and thus can also help in proper decision making
23. Conduct regular access control audits: An audit can identify any security weaknesses, such as unused accounts or overly permissive access, that need to be addressed.
24. Use access control tools and software: There are various access control tools and software available that can automate access management and provide centralized control over access permissions. Instead of a person being responsible of the access control, an automated software could also be helpful.
25. Conduct a data inventory: Conduct an inventory of all the data that the company collects and categorize it based on its sensitivity and importance.
26. Identify the access requirements for each type of data: Determine which employees need access to each type of data based on their job responsibilities.
27. Develop a policy document: Create a written policy document that outlines the access levels for each type of data and the requirements for accessing it.
28. Define access levels: Define the access levels, such as read-only, read-write, or admin, for each type of data.
29. Assign access levels: Assign access levels to each employee based on their job responsibilities and need to access each type of data.
30. Code obfuscation: This involves transforming the code into a form that is difficult to understand or reverse-engineer. This can include techniques such as renaming variables and functions, removing comments and whitespace, and splitting the code into multiple files.
31. Education and Training: Educate and train employees on the importance of data classification and marking. This can include providing information on how to identify sensitive data, the consequences of mishandling it, how to assign unique identification codes,
32. The organization should establish clear policies and procedures around data classification and marking.
33. Automated tools such as data classification software can help the organization automatically identify and classify sensitive data, reducing the likelihood of errors and ensuring that data is properly labeled. Automated systems such as barcoding or radio frequency identification (RFID) can help organizations automate the process of assigning and tracking unique identification codes.
34. The organization should establish clear standard operating procedures (SOPs) for assigning unique identification codes to products. This should include guidelines on how to create, assign, and track codes, as well as the consequences of failing to do so.
35. Establish an encryption policy that outlines the requirements for encryption of data at rest. This should include the type of encryption algorithm to be used, the minimum key length, and the scope of data that requires encryption.
36. Ensure that encryption keys are securely managed and stored separately from the encrypted data to prevent unauthorized access. This can include implementing multi-factor authentication and using hardware security modules (HSMs) for key storage.
37. Ensure that time period and lockout controls are properly configured and managed. This can include setting up automatic session timeouts, enforcing strong password policies, and configuring account lockout settings.
38. Continually review and improve time period and lockout controls based on feedback from users, audits, and security assessments. This can help ensure that controls remain effective and up-to-date with the latest security threats and vulnerabilities.
39. Use parameterized queries instead of dynamic queries to prevent command injection attacks. This can help ensure that user input is properly escaped and sanitized before being executed.
40. Implement the principle of least privilege to limit the amount of access that users have to the system or application. This can help prevent attackers from executing arbitrary commands even if they are able to exploit a vulnerability.
41. Conduct regular code reviews to identify and address any potential buffer overflow vulnerabilities in the code. This can include using automated tools to scan for potential vulnerabilities or manual reviews by experienced developers.
42. Implement memory protection techniques such as stack canaries, address space layout randomization (ASLR), and Data Execution Prevention (DEP) to prevent buffer overflows from being exploited.
43. Implementing the EAP-TTLS protocol, WPA3 protocol, SSID. This will help to ensure that the network is secure and that the users' credentials are protected.
44. Segmenting the network can help to isolate different areas of network, which can reduce the impact of a security breach. By segmenting the network, the organization can limit the access that an attacker has to the network, which can make it more difficult for them to exploit vulnerabilities.
45. The most effective way to prevent the risks associated with not implementing PIN/legacy pairing is to implement SSP, which is a more secure method of pairing Bluetooth devices. SSP provides stronger encryption and authentication mechanisms, making it more difficult for attackers to exploit vulnerabilities.
46. Strong Password Policies: Organizations should implement strong password policies, including password complexity requirements, expiration policies, and regular password changes. This can help to prevent unauthorized access to Bluetooth devices and reduce the risk of security breaches.
47. The most effective way to prevent the risks associated with not implementing anti-collision algorithms is to implement them in your RFID system. This will help to ensure that tags can communicate with reader without causing data loss or corruption.
48. Using multiple reader antennas can help to improve the coverage area of RFID system and reduce the risk of tag collisions. This can help to ensure that tags can communicate with reader without causing data loss or corruption.
49. The most effective way to prevent the risks associated with not implementing PIN or legacy pairing is to implement secure pairing methods such as Bluetooth Low Energy (BLE) or Near Field Communication (NFC) pairing. These methods provide stronger encryption and better protection against attacks compared to legacy pairing.
50. Disabling the broadcast of the SSID can make it more difficult for attackers to discover your wireless network. This will prevent casual attackers from finding the network, but it will not deter determined attackers who are using more advanced techniques.

**List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience (it is not required to write detailed policies) – Risk Response Strategy**

1. In the case of sensitive information disclosure, the organization needs to be prepared with a proper Business Continuity Plan (BCP) and Disaster Recovery (DR) plans and follow the mentioned strategies to contain the loss and understand what further action sot take to control the attack.
2. Installing stronger VPN (Virtual Private Networks), DMZ (Demilitarized Zones), strong firewalls, IDS and IPS (Intrusion Detection and Intrusion Prevention Systems) helps prevent attacks targeting the organizational networks
3. Incident Response Teams are must for all organizations as these teams have experts who help to contain the attack and further help to re-secure the networks
4. Regular training and simulations for incident response team members and other relevant employees need to be implemented to ensure they are prepared to respond to cyber security incidents.
5. The organization needs to incorporate processes for analyzing cyber security incidents and documenting findings and recommendations for future improvements to the incident response plan and controls.
6. In the case of survival of the company, the organization needs to be prepared with a proper Business Continuity Plan (BCP) and Disaster Recovery (DR) plans and follow the mentioned strategies to contain the loss and understand what further action sot take to control the attack.
7. Incident Response Teams are must for all organizations as these teams have experts who help to contain the attack and further help to re-secure the networks
8. In case of data loss, it is important to immediately access data from the other data centers and make the network functional without any availability delay to the customers.
9. It is always a good practice to record the incidents and also to the methodology of how the attack was contained and the necessary actions that were taken. These can help for any future references
10. It is important to make the Firewalls, IDS/IPS systems stronger after any incident. Investing in them will help any future incidents
11. Even in the times of an attack, it is important to continue supplying the services to the customer from a different source which is secure
12. In case of data loss, the database servers need to be contacted immediately to access data and make the network functional without any availability delay to the customers.
13. If there’s data loss or interception, responding quickly to contain the damage and minimize the impact on productivity is crucial. This needs to have a clear disaster recovery and business contingency plan in place for responding to data breaches or data loss incidents.
14. Incident Response Teams are must for all organizations as these teams have experts who help to contain the attack and further help to re-secure the networks
15. It is always a good practice to record the incidents and also to the methodology of how the attack was contained and the necessary actions that were taken. These can help for any future references
16. Even in the times of an attack, it is important to continue supplying the services to the customer from a different source which is secure
17. Implement network audit trails to track user activity and detect any unauthorized access attempts. This helps identify potential security breaches and ensures accountability and further prevent any such attempts
18. Mechanisms of Reverse-Engineering need to be established to prevent further attacks of similar kind. These help to track the attack for the tail to its head
19. Routers need to re-configured every time there’s a new type of attack
20. Network Access Control Lists (ACL) need to updated every time there’s a new type of attack to block any requests from the user that posed danger previously
21. Implement data loss prevention (DLP) tools: DLP tools can help prevent data theft by monitoring data access and usage patterns, identifying and blocking unauthorized attempts to access or transfer sensitive data.
22. Regularly backup data: Regularly backup data to ensure that data can be recovered in the event of a security incident or data loss.
23. Conduct vulnerability assessments: Conduct regular vulnerability assessments to identify potential weaknesses in the company's security posture.
24. Assign the DBA to also check and control the backup monitoring. This helps to ensure backup security and decreases the vulnerability
25. Assign a separate role to monitor the system state changes. This is necessary to track system performance and thus detecting unauthorized access.
26. Conduct regular security audits: Regularly audit security controls and practices to identify and address any vulnerabilities that could be exploited by attackers
27. If non-compliance is detected, the organization should take corrective action to address the issue. This can include retraining employees, revising policies and procedures, and implementing new controls to prevent similar incidents from occurring in the future.
28. In the event of a data breach or other security incident, the organizations\ should have an incident response plan in place that includes procedures for identifying and containing the incident, as well as notifying affected parties and mitigating any damage.
29. The organization should implement monitoring and auditing processes to detect any instances where SCI policies and procedures are not followed. This can include regular reviews of product tracking practices and audits of inventory systems to ensure that products are properly identified and tracked. Monitoring also needs to be done to detect any instances where encryption policies are not followed.
30. Implement regular data backups and store them in secure locations to ensure data recovery in case of a security incident or system failure.
31. Continually review and improve time period and lockout controls based on feedback from users, audits, and security assessments. This can help ensure that controls remain effective and up-to-date with the latest security threats and vulnerabilities.
32. Implement a patch management process to ensure that all systems and applications are kept up-to-date with the latest security patches and updates.
33. Network monitoring tools can help to identify potential security threats before they can be exploited. By monitoring the network, we can identify unusual activity and take action to prevent a security breach before it occurs.
34. Regular vulnerability scanning can help to identify potential vulnerabilities in the network that could be exploited by attackers. By identifying these vulnerabilities, we can take steps to address them before they can be exploited.
35. Implementing access controls such as strong passwords, multi-factor authentication, and user authentication policies can hel+p to prevent unauthorized access to your network.
36. Implementing encryption and authentication controls such as Secure Socket Layer (SSL) and Transport Layer Security (TLS) can help to ensure that Bluetooth communication is secure and that only authorized devices are able to connect.
37. Organizations should conduct regular system maintenance to ensure that their RFID systems are operating properly and that all components are up-to-date. This can help to prevent system failures and reduce the risk of security breaches.
38. Organizations should provide regular training and awareness programs for employees to ensure that they are aware of the security risks associated with RFID systems and understand how to use them securely. This can help to reduce the risk of human error and improve overall security posture.
39. Implement intrusion detection systems (IDS) and intrusion prevention systems (IPS) to monitor network traffic for any signs of unauthorized access or malicious activity.
40. Implement event logging and monitoring to track and investigate any security incidents that occur.
41. Implement an incident response plan that outlines the steps to be taken in the event of a security incident, including how to contain the incident and restore normal operations.
42. Conduct regular penetration testing to identify any vulnerabilities in the wireless network infrastructure that could be exploited.
43. Perform regular security audits to identify vulnerabilities in the network and address them before they can be exploited by attackers.
44. Limit Access: Limit access to Wi-Fi network to only authorized users. Consider using MAC address filtering or requiring user authentication to access the network.

**Applicable Government Regulations and Industry Standards**

1. **General Data Protection Regulation (GDPR):**

The General Data Protection Regulation (GDPR) is a regulation to strengthen data protection. Under the GDPR, personal data is defined as any information that can identify an individual directly or indirectly. This includes names, email addresses, phone numbers, IP addresses, and other personal identifiers. The GDPR sets out various rights for individuals whose personal data is being processed, including the right to access their data, the right to correct inaccurate data, the right to erasure, and the right to object to the processing of their data. To comply with the GDPR, companies are required to implement appropriate technical and organizational measures to comply with several principles, including:

1. Lawfulness, fairness, and transparency: Personal data must be processed lawfully, fairly, and in a transparent manner.
2. Purpose limitation: Personal data must be collected for specified, explicit, and legitimate purposes and not further processed in a manner that is incompatible with those purposes.
3. Data minimization: Personal data must be adequate, relevant, and limited to what is necessary in relation to the purposes for which it is processed.
4. Accuracy: Personal data must be accurate and kept up to date.
5. Storage limitation: Personal data must be kept in a form that permits identification of data subjects for no longer than is necessary for the purposes for which the personal data is processed.

It's worth noting that failure to comply with the GDPR can result in significant fines and penalties. Therefore, it's important for Larsen and Toubro - LTI to ensure that they are compliant with the GDPR if they process any personal data.

1. **Information Technology Act:**

The Information Technology Act is a law that governs electronic transactions, data protection, and digital signatures.

Under the Information Technology Act, 2000, companies that engage in electronic transactions or store electronic records are required to comply with certain provisions, including:

1. Digital signatures: The Act recognizes digital signatures as legally valid and provides a legal framework for their use in electronic transactions.
2. Data protection: The Act provides for the protection of personal information and imposes certain obligations to collect, process, store or transfer personal data. The Act also provides for penalties in the event of unauthorized access, disclosure, or destruction of such information.
3. Cybercrimes: The Act criminalizes certain activities related to electronic records and transactions, including hacking, identity theft, and cyberstalking. The Act also provides for penalties for such activities.
4. Intermediary liability: The Act provides a legal safe harbor for intermediaries that provide online services such as social media platforms, search engines, and e-commerce websites.
5. **Payment Card Industry Data Security Standard (PCI DSS):**

Since Larsen and Toubro – LTI stores payment card information it must comply with the Payment Card Industry Data Security Standard (PCI DSS).

PCI DSS is a set of security standards designed to ensure that Larsen and Toubro – LTI handles payment card data in a secure manner. The standard outlines a series of requirements that organizations must follow to protect payment card data, including:

1. Build and maintain a secure network and systems
2. Protect cardholder data
3. Maintain a vulnerability management program
4. Implement strong access control measures
5. Regularly monitor and test networks
6. Maintain an information security policy

To comply with PCI DSS, LTI must implement the necessary security controls to protect payment card data. This may include measures such as:

1. Encrypting payment card data in transit and at rest
2. Implementing access controls to limit access to payment card data
3. Regularly monitoring systems for unauthorized access or suspicious activity
4. Conducting regular vulnerability assessments and penetration testing
5. Maintaining strict policies and procedures for handling payment card data

By complying with PCI DSS, LTI can ensure that it is protecting its clients' payment card data and reducing the risk of data breaches or other security incidents. Failure to comply with PCI DSS can result in fines, legal liabilities, and damage to LTI's reputation.

1. **International Organization for Standardization (ISO) 9001:**

The International Organization for Standardization (ISO) 9001 is a standard that outlines best practices for quality management. It provides a framework for Larsen and Toubro – LTI to implement a quality management system (QMS) that can help them consistently meet customer and regulatory requirements and continually improve their products and services. Some ways in which ISO 9001 may apply to Larsen and Toubro Infotech (LTI):

1. Quality management system implementation: LTI can adopt the ISO 9001 standard to implement a QMS that is tailored to its business needs. The standard provides a framework for defining quality objectives, establishing processes to meet those objectives, and monitoring and measuring performance against those objectives.
2. Customer satisfaction: LTI can use the ISO 9001 standard to focus on meeting customer requirements and enhancing customer satisfaction. The standard emphasizes the importance of understanding customer needs, measuring customer satisfaction, and continually improving processes to meet customer expectations.
3. Continual improvement: ISO 9001 promotes a culture of continual improvement by requiring organizations to regularly assess their QMS and identify areas for improvement. LTI can use the standard to identify opportunities for improvement, implement corrective actions, and monitor the effectiveness of those actions.
4. Risk management: ISO 9001 requires organizations to identify and manage risks that may impact their ability to meet customer and regulatory requirements. LTI can use the standard to develop a risk management process that identifies and mitigates risks to its QMS and business processes.
5. Compliance: ISO 9001 can help LTI comply with applicable regulations and standards by providing a framework for implementing and maintaining a QMS that meets customer and regulatory requirements.
6. **International Organization for Standardization (ISO) 27001:**

ISO 27001 is a standard that outlines best practices for information security management. It provides a framework for managing and protecting sensitive information, including data privacy, cybersecurity, and risk management. As a global technology consulting and digital solutions company, LTI handles sensitive information on behalf of its clients. Therefore, ISO 27001 can be very relevant to LTI, especially if the company wants to demonstrate its commitment to information security.

By adopting ISO 27001, LTI can establish an Information Security Management System (ISMS) that can help identify and manage information security risks. This includes implementing security controls to protect information from unauthorized access, ensuring business continuity, and complying with legal and regulatory requirements related to information security. The certification process involves an audit by an independent certification body that verifies the implementation and effectiveness of the ISMS.

ISO 27001 certification can benefit LTI in several ways. Firstly, it can demonstrate to clients that LTI has taken steps to ensure the security and confidentiality of their information. This can be an important factor in winning and retaining client trust. Secondly, it can help LTI to improve its own internal information security practices and reduce the risk of security breaches or incidents. Finally, ISO 27001 certification can help LTI to comply with legal and regulatory requirements related to information security, especially in industries that have strict security requirements, such as healthcare or financial services. Overall, ISO 27001 can be a valuable framework for LTI to ensure that it has effective information security management practices in place, and to demonstrate its commitment to information security to clients and stakeholders.

**Ranking Table of Asset Risks across individual categories**

|  |  |
| --- | --- |
| **Category** | **Top 5 Asset Risks** |
| **Access Control Security Risk Management Implementation Controls and Policies** | 1. Disclosure of organizational data 2. Manipulations to data 3. Increase in attack probabilities 4. Lack of compliance 5. Operational failures |
| **Network Infrastructure Security Risk Management Implementation Controls and Policies** | 1. Loss of data and privacy 2. Pose danger to the survival of the organization 3. Losing access control 4. Costs and Efficiency 5. Exploit the organizational networks and devices |
| **Network Infrastructure Management Security Risk Management Implementation Controls and Policies** | 1. Network Congestion 2. Resource depletion 3. Privacy and Compliance violation 4. Business disruption 5. Reduced productivity |
| **Database Security Risk Management Implementation Controls and Policies** | 1. Insider Threat 2. Loss of reputation 3. Increased vulnerabilities to assets 4. Higher risk of error 5. Lack of balance in access control |
| **Applications Development Security Risk Management Implementation Controls and Policy** | 1. Higher likelihood of software bugs and errors 2. Increased brute force attacks 3. Increased denial of service attacks 4. Database attacks 5. Increase in malware attacks |
| **Wireless Security Risk Management Implementation Controls and Policies** | 1. Fraudulent activity 2. Network downtime 3. Legal and Compliance issues 4. Loss of productivity 5. Network congestion |

**Ranking Table of Vulnerability Risks across individual categories**

|  |  |
| --- | --- |
| **Category** | **Top 5 Vulnerability Risks** |
| **Access Control Security Risk Management Implementation Controls and Policies** | 1. Manual checking 2. Ease of unauthorized access 3. Ease of fooling the systems 4. Sensitive information disclosure 5. Social Engineering |
| **Network Infrastructure Security Risk Management Implementation Controls and Policies** | 1. Increase Attack surface 2. Increase in Cyber attacks 3. Data interception 4. Unknown data modifications/stealing of data 5. Difficulty in monitoring user activity |
| **Network Infrastructure Management Security Risk Management Implementation Controls and Policies** | 1. SYN Attacks flooding 2. Ease of VLAN access 3. Lack of port security 4. Interruption in operations 5. Lack of system security |
| **Database Security Risk Management Implementation Controls and Policies** | 1. Inconsistent access control 2. Theft 3. Higher risk of errors 4. Unknown data/file modifications 5. Limited traceability |
| **Applications Development Security Risk Management Implementation Controls and Policy** | 1. Malware infection 2. System crashes 3. Difficulty in implementing software testing processes 4. Lower rate of performance 5. Does not adhere to compliance |
| **Wireless Security Risk Management Implementation Controls and Policies** | 1. Increased Man-in-the-middle attacks 2. Identity spoofing 3. Denial of Service attacks 4. Difficulty in identifying networks 5. Interference with other networks |

**Ranking the Asset Risks across all categories**

1. Insider Threat
2. Increased denial of service attacks
3. Losing access control
4. Network Congestion
5. Disclosure of organizational data

**Ranking the Vulnerability Risks across all categories**

1. Increase Attack surface
2. Increased Man-in-the-middle attacks
3. Manual checking
4. Lack of port security
5. Difficulty in implementing software testing processes

**Cybersecurity Workforce Risk Management Implementation**

**List of Cybersecurity Specialty Areas that exist at Larsen and Toubro – LTI**

|  |
| --- |
| **Specialty Area** |
| Risk Management (RSK) |
| Software Development (DEV) |
| Systems Architecture (ARC) |
| Systems Requirements Planning (SRP) |
| Systems Development (SYS) |
| Knowledge Management (KMG) |
| Customer Service and Technical Support (STS) |
| Network Services (NET) |
| Legal Advice and Advocacy (LGA) |
| Training, Education, and Awareness (TEA) |
| Strategic Planning and Policy (SPP) |
| Program/Project Management (PMA) and Acquisition |
| Cybersecurity Defense Infrastructure Support (INF) |
| Incident Response (CIR) |
| Vulnerability Assessment and Management (VAM) |
| Exploitation Analysis (EXP) |
| Targets (TGT) |
| Cyber Operations (OPS) |
| Digital Forensics (FOR) |

**List of Cybersecurity Work Roles that exist at Larsen and Toubro – LTI**

|  |
| --- |
| **Work Role** |
| Authorizing Official/Designating Representative |
| Security Control Assessor |
| Software Developer |
| Secure Software Assessor |
| Enterprise Architect |
| Security Architect |
| Systems Requirements Planner |
| Information Systems Security Developer |
| Knowledge Manager |
| Technical Support Specialist |
| Network Operations Specialist |
| Cyber Legal Advisor |
| Privacy Officer/Privacy Compliance Manager |
| Cyber Instructional Curriculum Developer |
| Cyber Workforce Developer and Manager |
| Cyber Policy and Strategy Planner |
| Program Manager |
| Product Support Manager |
| IT Investment/Portfolio Manager |
| Cyber Defense Infrastructure Support Specialist |
| Cyber Defense Incident Responder |
| Vulnerability Assessment Analyst |
| Threat/Warning Analyst |
| Exploitation Analyst |
| Target Developer |
| Target Network Analyst |
| Cyber Operator |
| Law Enforcement /Counter Intelligence Forensics Analyst |
| Cyber Defense Forensics Analyst |

**List of Cybersecurity Tasks that exist at Larsen and Toubro – LTI**

|  |
| --- |
| **Tasks** |
| Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). |
| Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. |
| Establish acceptable limits for the software application, network, or system. |
| 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. |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. |
| Verify and update security documentation reflecting the application/system security design features. |
| Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. |
| Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. |
| Apply secure code documentation. |
| Consult with customers about software system design and maintenance. |
| Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct. |
| Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance. |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. |
| 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. |
| Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. |
| Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life. |
| Perform integrated quality assurance testing for security functionality and resiliency attack. |
| Develop secure software testing and validation procedures. |
| Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities. |
| 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. |
| 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. |
| Document and update as necessary all definition and architecture activities. |
| Integrate results regarding the identification of gaps in security architecture. |
| 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). |
| Employ secure configuration management processes. |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. |
| 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. |
| Consult with customers to evaluate functional requirements. |
| Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions. |
| Document a system's purpose and preliminary system security concept of operations. |
| Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware). |
| 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). |
| Develop detailed security design documentation for component and interface specifications to support system design and development. |
| Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications. |
| Provide support to security/certification test and evaluation activities. |
| Utilize models and simulations to analyze or predict system performance under different operating conditions. |
| 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. |
| Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization’s intellectual capital. |
| Promote knowledge sharing between information owners/users through an organization’s operational processes and systems. |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). |
| Troubleshoot system hardware and software. |
| Develop and deliver technical training to educate others or meet customer needs. |
| Administer accounts, network rights, and access to systems and equipment. |
| Monitor and report client-level computer system performance. |
| 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. |
| Monitor network capacity and performance. |
| Patch network vulnerabilities to ensure that information is safeguarded against outside parties. |
| Provide feedback on network requirements, including network architecture and infrastructure. |
| Evaluate the effectiveness of laws, regulations, policies, standards, or procedures. |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. |
| Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. |
| Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures. |
| 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. |
| Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. |
| Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations. |
| 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. |
| Support the design and execution of exercise scenarios. |
| Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. |
| Create training courses tailored to the audience and physical environment. |
| Design training curriculum and course content based on requirements. |
| Participate in development of training curriculum and course content. |
| 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. |
| Establish and maintain communication channels with stakeholders. |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. |
| Conduct learning needs assessments and identify requirements. |
| Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards. |
| Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields. |
| Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements. |
| 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. |
| Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. |
| Develop and maintain strategic plans. |
| Perform needs analysis to determine opportunities for new and improved business process solutions. |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. |
| Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training). |
| Lead and oversee budget, staffing, and contracting. |
| Perform needs analysis to determine opportunities for new and improved business process solutions. |
| Provide advice on project costs, design concepts, or design changes. |
| Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives. |
| Conduct import/export reviews for acquiring systems and software. |
| Review or conduct audits of information technology (IT) programs and projects. |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. |
| Draft and publish supply chain security and risk management documents. |
| Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications. |
| Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. |
| Build, install, configure, and test dedicated cyber defense hardware. |
| Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization). |
| Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them. |
| 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 initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. |
| Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). |
| Coordinate with intelligence analysts to correlate threat assessment data. |
| Write and publish after action reviews. |
| Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. |
| Coordinate incident response functions. |
| Conduct and/or support authorized penetration testing on enterprise network assets. |
| 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. |
| Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). |
| Identify threat tactics, and methodologies. |
| Identify intelligence gaps and shortfalls. |
| Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. |
| Monitor and report on validated threat activities. |
| Monitor open source websites for hostile content directed towards organizational or partner interests. |
| Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements. |
| Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. |
| Report intelligence-derived significant network events and intrusions. |
| Conduct and/or support authorized penetration testing on enterprise network assets. |
| Perform penetration testing as required for new or updated applications. |
| Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access. |
| Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access. |
| Monitor target networks to provide indications and warning of target communications changes or processing failures. |
| Produce network reconstructions. |
| Profile network or system administrators and their activities. |
| Determine what technologies are used by a given target. |
| Develop all-source intelligence targeting materials. |
| Develop measures of effectiveness and measures of performance. |
| Produce target system analysis products. |
| Provide aim point and reengagement recommendations. |
| Review appropriate information sources to determine validity and relevance of information gathered. |
| Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. |
| Identify and conduct analysis of target communications to identify information essential to support operations. |
| Conduct nodal analysis. |
| Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. |
| Identify collection gaps and potential collection strategies against targets. |
| Identify network components and their functionality to enable analysis and target development. |
| Provide target recommendations which meet leadership objectives. |
| Review appropriate information sources to determine validity and relevance of information gathered. |
| Analyze internal operational architecture, tools, and procedures for ways to improve performance. |
| Analyze target operational architecture for ways to gain access. |
| Conduct collection and processing of wireless computer and digital networks. |
| 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. |
| Maintain situational awareness and functionality of organic operational infrastructure. |
| Conduct cyber activities to degrade/remove information resident in computers and computer networks. |
| Test and evaluate locally developed tools for operational use. |
| Test internal developed tools and techniques against target tools. |
| Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. |
| Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals). |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. |
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. |
| Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. |
| Analyze organizational cyber policy. |
| Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. |
| Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. |
| 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 hash comparison against established database. |
| Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView). |
| Perform timeline analysis. |
| Perform virus scanning on digital media. |
| Perform file system forensic analysis. |
| Perform static analysis to mount an "image" of a drive (without necessarily having the original drive). |
| Perform static malware analysis. |
| Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. |
| Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information. |
| Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies. |

**Comparison of the NCWF recommended Cybersecurity Specialty Areas with Larsen and Toubro – LTI’s existing Cybersecurity Specialty Areas**

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

**Comparison of the NCWF recommended Cybersecurity Work Roles with Larsen and Toubro – LTI’s existing Cybersecurity Work Roles**

|  |  |
| --- | --- |
| **Work Roles** | **Status** |
| Authorizing Official/Designating Representative | Present |
| Security Control Assessor | Present |
| Software Developer | Present |
| Secure Software Assessor | Present |
| Enterprise Architect | Present |
| Security Architect | Present |
| Research & Development Specialist | Absent |
| Systems Requirements Planner | Present |
| System Testing and Evaluation Specialist | Absent |
| Information Systems Security Developer | Present |
| Systems Developer | Absent |
| Database Administrator | Absent |
| Data Analyst | Absent |
| Knowledge Manager | Present |
| Technical Support Specialist | Present |
| Network Operations Specialist | Present |
| System Administrator | Absent |
| System Security Analyst | Absent |
| Cyber Legal Advisor | Present |
| Privacy Officer/Privacy Compliance Manager | Present |
| Cyber Instructional Curriculum Developer | Present |
| Cyber Instructor | Absent |
| Information Systems Security Manager | Absent |
| Communications Security (COMSEC) Manager | Absent |
| Cyber Workforce Developer and Manager | Present |
| Cyber Policy and Strategy Planner | Present |
| Executive Cyber Leadership | Absent |
| Program Manager | Present |
| IT Project Manager | Absent |
| Product Support Manager | Present |
| IT Investment/Portfolio Manager | Present |
| IT Program Auditor | Absent |
| Cyber Defense Analyst | Absent |
| Cyber Defense Infrastructure Support Specialist | Present |
| Cyber Defense Incident Responder | Present |
| Vulnerability Assessment Analyst | Present |
| Threat/Warning Analyst | Present |
| Exploitation Analyst | Present |
| All-Source Analyst | Absent |
| Mission Assessment Specialist | Absent |
| Target Developer | Present |
| Target Network Analyst | Present |
| Multi-Disciplined Language Analyst | Absent |
| All-Source Collection Manager | Absent |
| All-Source Collection Requirements Manager | Absent |
| Cyber Intel Planner | Absent |
| Cyber Ops Planner | Absent |
| Partner Integration Planner | Absent |
| Cyber Operator | Present |
| Cyber Crime Investigator | Absent |
| Law Enforcement /Counter Intelligence Forensics Analyst | Present |
| Cyber Defense Forensics Analyst | Present |

**Comparison the NCWF recommended Cybersecurity Tasks with Larsen and Toubro – LTI’s existing Cybersecurity Tasks**

|  |  |
| --- | --- |
| **Tasks** | **Status** |
| 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). | Absent |
| Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). | Absent |
| Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks. | Absent |
| 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 centers). | Present |
| Establish acceptable limits for the software application, network, or system. | Present |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). | Absent |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. | Present |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. | Absent |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Absent |
| Verify and update security documentation reflecting the application/system security design features. | 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. | Absent |
| Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment. | Absent |
| Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. | Present |
| Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Assess the effectiveness of security controls. | Absent |
| Assess all the configuration management (change configuration/release management) processes. | Absent |
| Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application. | Absent |
| Analyze 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. | Present |
| Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules. | Absent |
| 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. | Absent |
| 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. | Absent |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Absent |
| Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language. | Absent |
| Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. | Absent |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Absent |
| Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria. | Absent |
| Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements. | Absent |
| Identify and leverage the enterprise-wide version control system while designing and developing secure applications. | Absent |
| Consult with customers about software system design and maintenance. | Absent |
| Direct software programming and development of documentation. | 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. | Absent |
| Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate. | Absent |
| Conduct trial runs of programs and software applications to ensure that the desired information is produced, and instructions and security levels are correct. | Present |
| Develop software system testing and validation procedures, programming, and documentation. | Absent |
| Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance. | 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. | Absent |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. | Absent |
| Apply secure code documentation. | 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 |
| Develop threat model based on customer interviews and requirements. | Present |
| Consult with engineering staff to evaluate interface between hardware and software. | Absent |
| Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. | Absent |
| Identify basic common coding flaws at a high level. | Absent |
| Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. | 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. | Present |
| Perform integrated quality assurance testing for security functionality and resiliency attack. | Present |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Absent |
| Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. | Absent |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Absent |
| Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria. | Absent |
| Perform penetration testing as required for new or updated applications. | Absent |
| Consult with customers about software system design and maintenance. | Absent |
| Direct software programming and development of documentation. | Absent |
| Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Absent |
| Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application. | Absent |
| Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates. | Absent |
| Conduct trial runs of programs and software applications to ensure that the desired information is produced, and instructions and security levels are correct. | Absent |
| Develop secure software testing and validation procedures. | Present |
| Develop system testing and validation procedures, programming, and documentation. | Absent |
| Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities. | Present |
| Determine and document software patches or the extent of releases that would leave software vulnerable. | 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 |
| Employ secure configuration management processes. | Absent |
| Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. | Absent |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. | Absent |
| Provide advice on project costs, design concepts, or design changes. | Present |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Present |
| Analyze candidate architectures, allocate security services, and select security mechanisms. | Present |
| Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | Absent |
| Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. | Present |
| Write detailed functional specifications that document the architecture development process. | Absent |
| Analyze user needs and requirements to plan architecture. | Absent |
| Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. | Absent |
| Develop enterprise architecture or system components required to meet user needs. | Absent |
| Document and update as necessary all definition and architecture activities. | Present |
| Integrate results regarding the identification of gaps in security architecture. | Present |
| Plan implementation strategy to ensure that enterprise components can be integrated and aligned. | Absent |
| Translate proposed capabilities into technical requirements. | Absent |
| Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture. | Absent |
| Integrate key management functions as related to cyberspace. | Absent |
| 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. | Present |
| Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET). | Present |
| Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle. | Absent |
| Employ secure configuration management processes. | Present |
| 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. | Present |
| Provide advice on project costs, design concepts, or design changes. | Absent |
| Provide input on security requirements to be included in statements of work and other appropriate procurement documents. | 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 |
| Analyze candidate architectures, allocate security services, and select security mechanisms. | Absent |
| Develop a system security context, a preliminary system security Concept of Operations (CONOPS) and define baseline system security requirements in accordance with applicable cybersecurity requirements. | Present |
| Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. | Absent |
| Write detailed functional specifications that document the architecture development process. | Absent |
| Analyze user needs and requirements to plan architecture. | Absent |
| Develop enterprise architecture or system components required to meet user needs. | Absent |
| Document and update as necessary all definition and architecture activities. | 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 |
| 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 |
| Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications. | Absent |
| Consult with customers to evaluate functional requirements. | 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. | Absent |
| Develop and document requirements, capabilities, and constraints for design procedures and processes. | Absent |
| Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements. | Absent |
| Oversee and make recommendations regarding configuration management. | Absent |
| Perform needs analysis to determine opportunities for new and improved business process solutions. | Absent |
| Prepare use cases to justify the need for specific information technology (IT) solutions. | Absent |
| Translate functional requirements into technical solutions. | Absent |
| Develop and document supply chain risks for critical system elements, as appropriate. | Absent |
| Develop and document User Experience (UX) requirements including information architecture and user interface requirements. | Absent |
| Design and document quality standards. | Absent |
| Document a system's purpose and preliminary system security concept of operations. | 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 |
| Determine level of assurance of developed capabilities based on test results. | Absent |
| Develop test plans to address specifications and requirements. | Absent |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Absent |
| Make recommendations based on test results. | Absent |
| Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated. | Absent |
| Create auditable evidence of security measures. | Absent |
| Validate specifications and requirements for testability. | Absent |
| Analyze the results of software, hardware, or interoperability testing. | Absent |
| Perform developmental testing on systems under development. | Absent |
| Perform interoperability testing on systems exchanging electronic information with other systems. | Absent |
| Perform operational testing. | Absent |
| Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements. | Absent |
| Record and manage test data. | Absent |
| Analyze design constraints, analyze 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. | Present |
| Assess the effectiveness of cybersecurity measures utilized by system(s). | Present |
| Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile. | Absent |
| Build, test, and modify product prototypes using working models or theoretical models. | Absent |
| Conduct Privacy Impact Assessments (PIAs) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII). | Absent |
| Design and develop cybersecurity or cybersecurity-enabled products. | Absent |
| Design hardware, operating systems, and software applications to adequately address cybersecurity requirements. | Absent |
| Design or integrate appropriate data backup capabilities into overall system designs and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data. | Absent |
| Develop and direct system testing and validation procedures and documentation. | Absent |
| Develop detailed security design documentation for component and interface specifications to support system design and development. | Present |
| Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | 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. | Present |
| Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements. | Absent |
| Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find workarounds 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. | Present |
| Utilize models and simulations to analyze or predict system performance under different operating conditions. | Present |
| Design and develop key management functions (as related to cybersecurity). | Absent |
| Analyze user needs and requirements to plan and conduct system security development. | Absent |
| Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information). | Absent |
| Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary. | Absent |
| Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment. | Absent |
| Employ configuration management processes. | Absent |
| Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. | Absent |
| Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation. | Absent |
| Design to security requirements to ensure requirements are met for all systems and/or applications. | 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 |
| Analyze design constraints, analyze 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 analyze or predict system performance under different operating conditions. | Absent |
| Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment. | Absent |
| Employ configuration management processes. | Absent |
| Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements. | Absent |
| Design and develop system administration and management functionality for privileged access users. | Absent |
| Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies. | Absent |
| Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle). | Absent |
| Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary. | Absent |
| Design hardware, operating systems, and software applications to adequately address requirements. | Absent |
| Design to security requirements to ensure requirements are met for all systems and/or applications. | Absent |
| Develop detailed design documentation for component and interface specifications to support system design and development. | Absent |
| Develop mitigation strategies to address cost, schedule, performance, and security risks. | Absent |
| Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements. | Absent |
| Implement designs for new or existing system(s). | Absent |
| Perform security reviews and identify security gaps in architecture. | Absent |
| Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials | Absent |
| Provide support to test and evaluation activities. | Absent |
| Trace system requirements to design components and perform gap analysis. | Absent |
| Verify stability, interoperability, portability, and/or scalability of system architecture. | Absent |
| Analyze user needs and requirements to plan and conduct system development. | Absent |
| Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations. | 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 |
| Analyze and plan for anticipated changes in data capacity requirements. | Absent |
| Maintain database management systems software. | Absent |
| Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing. | Absent |
| Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required. | Absent |
| Manage the compilation, cataloging, caching, distribution, and retrieval of data. | Absent |
| Monitor and maintain databases to ensure optimal performance. | Absent |
| Perform backup and recovery of databases to ensure data integrity. | Absent |
| Provide recommendations on new database technologies and architectures. | Absent |
| Performs configuration management, problem management, capacity management, and financial management for databases and data management systems. | Absent |
| Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems. | Absent |
| Maintain assured message delivery systems. | Absent |
| Implement data management standards, requirements, and specifications. | Absent |
| Implement data mining and data warehousing applications. | Absent |
| Install and configure database management systems and software. | Absent |
| Analyze and define data requirements and specifications. | Absent |
| Analyze and plan for anticipated changes in data capacity requirements. | Absent |
| Develop data standards, policies, and procedures. | Absent |
| Manage the compilation, cataloging, caching, distribution, and retrieval of data. | 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 |
| Analyze data sources to provide actionable recommendations. | Absent |
| Assess the validity of source data and subsequent findings. | Absent |
| Collect metrics and trending data. | Absent |
| Conduct hypothesis testing using statistical processes. | Absent |
| Confer with systems analysts, engineers, programmers, and others to design application. | Absent |
| Develop and facilitate data-gathering methods. | 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 |
| Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users. | Absent |
| Develop an understanding of the needs and requirements of information end-users. | Present |
| Monitor and report the usage of knowledge management assets and resources. | Present |
| Plan and manage the delivery of knowledge management projects. | Present |
| Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information. | 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. | Present |
| Promote knowledge sharing between information owners/users through an organization’s operational processes and systems. | Present |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Present |
| Troubleshoot system hardware and software. | Present |
| Analyze incident data for emerging trends. | Absent |
| Develop and deliver technical training to educate others or meet customer needs. | Present |
| Maintain incident tracking and solution database. | Absent |
| Diagnose and resolve customer reported system incidents, problems, and events. | Absent |
| Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience. | Absent |
| Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards. | Absent |
| Administer accounts, network rights, and access to systems and equipment. | Present |
| Perform asset management/inventory of information technology (IT) resources. | Absent |
| Monitor and report client-level computer system performance. | Present |
| Develop a trend analysis and impact report. | Absent |
| Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling). | 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. | Absent |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Absent |
| Install or replace network hubs, routers, and switches. | Absent |
| Integrate new systems into existing network architecture. | Absent |
| Monitor network capacity and performance. | Present |
| Patch network vulnerabilities to ensure that information is safeguarded against outside parties. | Present |
| Provide feedback on network requirements, including network architecture and infrastructure. | Present |
| Test and maintain network infrastructure including software and hardware devices. | Absent |
| Conduct functional and connectivity testing to ensure continuing operability. | Absent |
| Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs. | Absent |
| Develop and document systems administration standard operating procedures. | Absent |
| Maintain baseline system security according to organizational policies. | Absent |
| Manage accounts, network rights, and access to systems and equipment. | Absent |
| Plan, execute, and verify data redundancy and system recovery procedures. | Absent |
| Provide ongoing optimization and problem-solving support. | Absent |
| Install, update, and troubleshoot systems/servers. | Absent |
| Check system hardware availability, functionality, integrity, and efficiency. | Absent |
| Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing. | Absent |
| Comply with organization systems administration standard operating procedures. | Absent |
| Implement and enforce local network usage policies and procedures. | Absent |
| Manage system/server resources including performance, capacity, availability, serviceability, and recoverability. | Absent |
| Monitor and maintain system/server configuration. | Absent |
| Oversee installation, implementation, configuration, and support of system components. | Absent |
| Diagnose faulty system/server hardware. | Absent |
| Perform repairs on faulty system/server hardware. | Absent |
| Troubleshoot hardware/software interface and interoperability problems. | Absent |
| Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications. | Absent |
| Apply security policies to meet security objectives of the system. | Absent |
| Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements. | Absent |
| Ensure all systems security operations and maintenance activities are properly documented and updated as necessary. | Absent |
| Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment. | Absent |
| Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. | Absent |
| Implement specific cybersecurity countermeasures for systems and/or applications. | Absent |
| Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system. | Absent |
| Perform cybersecurity testing of developed applications and/or systems. | Absent |
| 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. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Absent |
| Verify and update security documentation reflecting the application/system security design features. | Absent |
| Assess the effectiveness of security controls. | Absent |
| Assess all the configuration management (change configuration/release management) processes. | Absent |
| Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements. | Absent |
| Analyze and report organizational security posture trends. | Absent |
| Analyze and report system security posture trends. | Absent |
| Assess adequate access controls based on principles of least privilege and need-to-know. | Absent |
| Ensure the execution of disaster recovery and continuity of operations. | Absent |
| Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed. | Absent |
| Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation. | Absent |
| Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment. | Absent |
| Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative. | Absent |
| Assess and monitor cybersecurity related to system implementation and testing practices. | 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. | Absent |
| Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. | Absent |
| 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. | Present |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| 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. | Present |
| Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures. | Present |
| Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery). | Absent |
| 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). | Present |
| Develop and maintain strategic plans. | Present |
| Evaluate contracts to ensure compliance with funding, legal, and program requirements. | Present |
| 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. | Present |
| Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations. | Present |
| Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements. | Present |
| Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner. | Absent |
| Liaise with regulatory and accrediting bodies. | Absent |
| Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues. | Absent |
| Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance. | 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 |
| Support the design and execution of exercise scenarios. | Present |
| Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. | 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 |
| 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. | Present |
| 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. | Present |
| Participate in development of training curriculum and course content. | Present |
| Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness. | 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. | Present |
| 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., 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 |
| Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture. | Absent |
| Collect and maintain data needed to meet system cybersecurity reporting. | Absent |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Absent |
| Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. | Absent |
| Ensure that security improvement actions are evaluated, validated, and implemented as required. | Absent |
| Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment. | Absent |
| Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s). | Absent |
| Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture. | Absent |
| Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy. | Absent |
| Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed. | Absent |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Absent |
| Identify alternative information security strategies to address organizational security objective. | Absent |
| Identify information technology (IT) security program implications of new technologies or technology upgrades. | Absent |
| Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information. | Absent |
| Interpret and/or approve security requirements relative to the capabilities of new information technologies. | Absent |
| Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program. | 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 monitoring of information security data sources to maintain organizational situational awareness. | Absent |
| Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. | Absent |
| Manage threat or target analysis of cyber defense information and production of threat information within the enterprise. | Absent |
| Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. | Absent |
| Oversee the information security training and awareness program. | Absent |
| Participate in an information security risk assessment during the Security Assessment and Authorization process. | Absent |
| Participate in the development or modification of the computer environment cybersecurity program plans and requirements. | Absent |
| Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations. | Absent |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | Absent |
| Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities. | Absent |
| Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents. | Absent |
| Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters. | Absent |
| Recognize a possible security violation and take appropriate action to report the incident, as required. | Absent |
| Recommend resource allocations required to securely operate and maintain an organization’s cybersecurity requirements. | Absent |
| Recommend policy and coordinate review and approval. | Absent |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Absent |
| Track audit findings and recommendations to ensure that appropriate mitigation actions are taken. | Absent |
| Use federal and organization-specific published documents to manage operations of their computing environment system(s). | 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 |
| Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk. | Absent |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Absent |
| Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. | Absent |
| Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. | Absent |
| Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals. | Absent |
| Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs). | Absent |
| Participate in the acquisition process as necessary, following appropriate supply chain risk management practices. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance. | Absent |
| Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary. | Absent |
| Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate. | Absent |
| Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. | Absent |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Absent |
| Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. | Absent |
| Ensure that security improvement actions are evaluated, validated, and implemented as required. | Absent |
| Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy. | Absent |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Absent |
| Recognize a possible security violation and take appropriate action to report the incident, as required. | Absent |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Absent |
| 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. | Present |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Present |
| 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. | Present |
| Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards. | Present |
| 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. | Present |
| Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements. | Present |
| 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 |
| Analyze organizational cyber policy. | Absent |
| Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. | Absent |
| Correlate training and learning to business or mission requirements. | Absent |
| Define and integrate current and future mission environments. | Absent |
| Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan. | Absent |
| Draft, staff, and publish cyber policy. | Absent |
| Identify and address cyber workforce planning and management issues (e.g., recruitment, retention, and training). | Absent |
| Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. | Absent |
| Seek consensus on proposed policy changes from stakeholders. | Absent |
| Provide policy guidance to cyber management, staff, and users. | Absent |
| Review, conduct, or participate in audits of cyber programs and projects. | Absent |
| Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media). | Absent |
| Support the CIO in the formulation of cyber-related policies. | Absent |
| Review and approve a supply chain security/risk management policy. | Absent |
| 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. | Present |
| Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. | Present |
| Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. | Absent |
| Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. | Absent |
| Analyze organizational cyber policy. | Absent |
| Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. | Absent |
| Define and integrate current and future mission environments. | Absent |
| Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan. | Absent |
| Draft, staff, and publish cyber policy. | Absent |
| Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services. | Present |
| 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 |
| 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. | Present |
| Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information. | Absent |
| Lead and align information technology (IT) security priorities with the security strategy. | Absent |
| Lead and oversee information security budget, staffing, and contracting. | Absent |
| Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. | Absent |
| Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. | Absent |
| Recommend policy and coordinate review and approval. | Absent |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Absent |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Absent |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. | Absent |
| Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. | Absent |
| Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle. | Absent |
| Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc. | Absent |
| Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate. | Absent |
| Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Absent |
| Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. | Absent |
| Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities. | Absent |
| Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan. | Absent |
| Perform an information security risk assessment. | Absent |
| Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| Collaborate on cyber privacy and security policies and procedures | Absent |
| Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation | Absent |
| Appoint and guide a team of IT security experts. | Absent |
| Collaborate with key stakeholders to establish a cybersecurity risk management program. | Absent |
| Develop and maintain strategic plans. | Absent |
| 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. | 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. | 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. | Present |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Absent |
| Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction, and monitor all significant activities so the service is delivered successfully. | Absent |
| Coordinate and manage the overall service provided to a customer end-to-end. | Absent |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Absent |
| Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). | Absent |
| Participate in the acquisition process as necessary. | Absent |
| Conduct import/export reviews for acquiring systems and software. | Absent |
| Develop supply chain, system, network, performance, and cybersecurity requirements. | Absent |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Absent |
| Identify and address cyber workforce planning and management issues (e.g., recruitment, retention, and training). | Present |
| Lead and oversee budget, staffing, and contracting. | Present |
| Draft and publish supply chain security and risk management documents. | Absent |
| 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. | 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. | Absent |
| Provide ongoing optimization and problem-solving support. | Absent |
| Provide recommendations for possible improvements and upgrades. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Absent |
| Develop and document supply chain risks for critical system elements, as appropriate. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully. | Absent |
| Coordinate and manage the overall service provided to a customer end-to-end. | Absent |
| Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service. | Absent |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Absent |
| Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs). | Absent |
| Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. | Absent |
| Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives. | Present |
| Participate in the acquisition process as necessary. |  |
| Conduct import/export reviews for acquiring systems and software. | Present |
| Develop supply chain, system, network, performance, and cybersecurity requirements. | Absent |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Absent |
| Identify and address cyber workforce planning and management issues (e.g., recruitment, retention, and training). | Absent |
| Lead and oversee budget, staffing, and contracting. | Absent |
| Draft and publish supply chain security and risk management documents. | Absent |
| 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. | Present |
| 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. | Present |
| 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. | Present |
| Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. | Absent |
| 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. | Present |
| Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Absent |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Absent |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Absent |
| Lead and oversee budget, staffing, and contracting. | Absent |
| Draft and publish supply chain security and risk management documents. | Absent |
| 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 |
| Develop content for cyber defense tools. | Absent |
| Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources. | Absent |
| Coordinate with enterprise-wide cyber defense staff to validate network alerts. | Present |
| Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. | Absent |
| Document and escalate incidents (including event’s history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment. | Absent |
| Perform cyber defense trend analysis and reporting. | Absent |
| Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | Absent |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. | Absent |
| Plan and recommend modifications or adjustments based on exercise results or system environment. | Absent |
| Provide daily summary reports of network events and activity relevant to cyber defense practices. | Absent |
| Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. | 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 defense tools for continual monitoring and analysis of system activity to identify malicious activity. | Absent |
| Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. | Absent |
| Determine tactics, techniques, and procedures (TTPs) for intrusion sets. | Absent |
| Examine network topologies to understand data flows through the network. | Absent |
| Recommend computing environment vulnerability corrections. | Absent |
| Identify and analyze anomalies in network traffic using metadata. | Absent |
| Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings). | Absent |
| Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools. | 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 defense network tools in response to new or observed threats within the network environment or enclave. | Absent |
| Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan. | Absent |
| Analyze and report organizational security posture trends. | Absent |
| Analyze and report system security posture trends. | Absent |
| Assess adequate access controls based on principles of least privilege and need-to-know. | Absent |
| Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. | Absent |
| Assess and monitor cybersecurity related to system implementation and testing practices. | Absent |
| Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities. | Absent |
| Work with stakeholders to resolve computer security incidents and vulnerability compliance. | Absent |
| Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans. | Absent |
| Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications. | Absent |
| Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit, and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration. | Present |
| Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources. | Absent |
| Build, install, configure, and test dedicated cyber defense hardware. | Present |
| Assist in assessing the impact of implementing and sustaining a dedicated cyber defense 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 defense systems (e.g., firewalls and intrusion prevention systems). | Absent |
| Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization). | Present |
| Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them. | Present |
| Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. | Absent |
| Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. | Absent |
| Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security. | Present |
| Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. | Absent |
| Perform cyber defense trend analysis and reporting. |  |
| Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. | Present |
| Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). | Present |
| Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. | Absent |
| Track and document cyber defense incidents from initial detection through final resolution. | Absent |
| Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. | Absent |
| Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness). | Absent |
| Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. | Absent |
| Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. | Absent |
| Coordinate with intelligence analysts to correlate threat assessment data. | Present |
| Write and publish after action reviews. | Present |
| Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise. | Present |
| Coordinate incident response functions. | Present |
| 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. | Present |
| Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. | Present |
| Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. | Absent |
| 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). | Absent |
| Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). | Absent |
| Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). | Present |
| 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. | Present |
| Identify intelligence gaps and shortfalls. | Present |
| Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. | Present |
| Monitor and report on validated threat activities. | Present |
| Monitor open-source websites for hostile content directed towards organizational or partner interests. | Present |
| Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements. | Present |
| Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Present |
| Provide current intelligence support to critical internal/external stakeholders as appropriate. | Absent |
| Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. | Absent |
| Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. | Absent |
| Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations. | Absent |
| Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities. | Absent |
| Report intelligence-derived significant network events and intrusions. | Present |
| Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date. | Absent |
| Conduct and/or support authorized penetration testing on enterprise network assets. | Present |
| Perform penetration testing as required for new or updated applications. | Present |
| 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. | Present |
| Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access. | Present |
| 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. | Present |
| Produce network reconstructions. | Present |
| Profile network or system administrators and their activities. | Present |
| 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 |
| Provide expertise to course of action development. | Absent |
| Provide subject matter expertise to the development of a common operational picture. | Absent |
| Provide subject matter expertise to the development of cyber operations specific indicators. | Absent |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Absent |
| Provide expertise to the development of measures of effectiveness and measures of performance. | Absent |
| Assist in the identification of intelligence collection shortfalls. | Absent |
| Brief threat and/or target current situations. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Conduct end-of-operations assessments. | Absent |
| Conduct in-depth research and analysis. | Absent |
| Conduct nodal analysis. | Absent |
| Conduct target research and analysis. | Absent |
| Develop information requirements necessary for answering priority information requests. | Absent |
| Develop measures of effectiveness and measures of performance. | Absent |
| Develop munitions effectiveness assessment or operational assessment materials. | Absent |
| Engage customers to understand customers’ intelligence needs and wants. | Absent |
| Estimate operational effects generated through cyber activities. | Absent |
| Evaluate threat decision-making processes. | Absent |
| Identify threat vulnerabilities. | Absent |
| Generate requests for information. | Absent |
| Identify intelligence gaps and shortfalls. | Absent |
| Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. | Absent |
| Monitor and report on validated threat activities. | Absent |
| Monitor operational environment and report on adversarial activities which fulfill leadership’s priority information requirements. | Absent |
| Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies). | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| Provide analyses and support for effectiveness assessment. | Absent |
| Provide current intelligence support to critical internal/external stakeholders as appropriate. | Absent |
| Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. | Absent |
| Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations. | Absent |
| Provide input and assist in post-action effectiveness assessments. | Absent |
| Provide input and assist in the development of plans and guidance. | Absent |
| Provide effectiveness support to designated exercises, and/or time sensitive operations. | Absent |
| Provide target recommendations which meet leadership objectives. | Absent |
| Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date. | Absent |
| 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. | Present |
| 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 |
| 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. | Present |
| Identify and conduct analysis of target communications to identify information essential to support operations. | Present |
| Conduct nodal analysis. | Present |
| Conduct quality control to determine validity and relevance of information gathered about networks. | 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. | Present |
| Identify collection gaps and potential collection strategies against targets. | Present |
| Identify network components and their functionality to enable analysis and target development. | Present |
| Make recommendations to guide collection in support of customer requirements. | Absent |
| Provide subject matter expertise to development of exercises. | Present |
| 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. | Present |
| 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 |
| Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. | Absent |
| Determine what technologies are used by a given target. | Absent |
| Identify collection gaps and potential collection strategies against targets. | Absent |
| Make recommendations to guide collection in support of customer requirements. | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| Advise managers and operators on language and cultural issues that impact organization objectives. | Absent |
| Analyze and process information using language and/or cultural expertise. | Absent |
| Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities. | Absent |
| Collaborate across internal and/or external organizational lines to enhance collection, analysis, and dissemination. | Absent |
| Conduct all-source target research to include the use of open source materials in the target language. | Absent |
| Conduct analysis of target communications to identify essential information in support of organization objectives. | Absent |
| Perform quality review and provide feedback on transcribed or translated materials. | Absent |
| Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing. | Absent |
| Identify cyber threat tactics and methodologies. | Absent |
| Identify target communications within the global network. | Absent |
| Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis. | Absent |
| Provide feedback to collection managers to enhance future collection and analysis. | Absent |
| Perform foreign language and dialect identification in initial source data. | Absent |
| Perform or support technical network analysis and mapping. | Absent |
| Provide requirements and feedback to optimize the development of language processing tools. | Absent |
| Perform social network analysis and document as appropriate. | Absent |
| Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material. | Absent |
| Tip critical or time-sensitive information to appropriate customers. | Absent |
| Transcribe target voice materials in the target language. | Absent |
| Translate (e.g., verbatim, gist, and/or summaries) target graphic material. | Absent |
| Translate (e.g., verbatim, gist, and/or summaries) target voice material. | Absent |
| Identify foreign language terminology within computer programs (e.g., comments, variable names). | Absent |
| Provide near-real time language analysis support (e.g., live operations). | Absent |
| Identify cyber/technology-related terminology in the target language. | Absent |
| Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements. | Absent |
| Analyze feedback to determine extent to which collection products and services are meeting requirements. | Absent |
| Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and 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 |
| Analyze feedback to determine extent to which collection products and services are meeting requirements. | Absent |
| Analyze incoming collection requests. | Absent |
| Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and 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 centers. | Absent |
| Disseminate reports to inform decision makers on collection issues. | Absent |
| Conduct and document an assessment of the collection results using established procedures. | Absent |
| Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership. | Absent |
| Evaluate extent to which collected information and/or produced intelligence satisfy information requests. | Absent |
| Evaluate extent to which collection operations are synchronized with operational requirements. | Absent |
| Evaluate the effectiveness of collection operations against the collection plan. | Absent |
| Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups. | Absent |
| Identify and mitigate risks to collection management ability to support the plan, operations and target cycle. | Absent |
| Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures. | Absent |
| Issue requests for information. | Absent |
| Modify collection requirements as necessary. | Absent |
| Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans. | Absent |
| Review capabilities of allocated collection assets. | Absent |
| Review intelligence collection guidance for accuracy/applicability. | Absent |
| Review list of prioritized collection requirements and essential information. | Absent |
| Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements. | Absent |
| Submit information requests to collection requirement management section for processing as collection requests. | Absent |
| Track status of information requests, including those processed as collection requests and production requirements, using established procedures. | Absent |
| Translate collection requests into applicable discipline-specific collection requirements. | Absent |
| Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness. | Absent |
| Validate requests for information according to established criteria. | Absent |
| 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 |
| Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives. | Absent |
| Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement. | 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 |
| Provide input to the identification of cyber-related success criteria. | Absent |
| Develop, review and implement all levels of planning guidance in support of cyber operations. | Absent |
| Contribute to crisis action planning for cyber operations. | Absent |
| Contribute to the development of the organization's decision support tools if necessary. | Absent |
| Coordinate with intelligence and cyber defense partners to obtain relevant essential information. | 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 maintain deliberate and/or crisis plans. | Absent |
| Develop and review specific cyber operations guidance for integration into broader planning activities. | Absent |
| Develop cyber operations plans and guidance to ensure that execution and resource allocation decisions align with organization objectives. | 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 potential courses of action. | Absent |
| Develop, implement, and recommend changes to appropriate planning procedures and policies. | Absent |
| Devise, document, and validate cyber operation strategy and planning documents. | Absent |
| Ensure operational planning efforts are effectively transitioned to current operations. | Absent |
| Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines. | Absent |
| Evaluate intelligence estimates to support the planning cycle. | Absent |
| Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives. | Absent |
| Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities. | Absent |
| Incorporate cyber operations and communications security support plans into organization objectives. | Absent |
| Identify cyber intelligence gaps and shortfalls for cyber operational planning. | Absent |
| Integrate cyber planning/targeting efforts with other organizations. | Absent |
| Interpret environment preparations assessments to determine a course of action. | Absent |
| Issue requests for information. | Absent |
| Maintain relationships with internal and external partners involved in cyber planning or related areas. | Absent |
| Maintain situational awareness of cyber-related intelligence requirements and associated tasking. | Absent |
| Maintain situational awareness of partner capabilities and activities. | Absent |
| Maintain situational awareness to determine if changes to the operating environment require review of the plan. | Absent |
| Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives. | Absent |
| Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| Provide subject matter expertise to planning efforts with internal and external cyber operations partners. | Absent |
| Prepare for and provide subject matter expertise to exercises. | Absent |
| Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs. | Absent |
| Provide input to the administrative and logistical elements of an operational support plan. | Absent |
| Provide planning support between internal and external partners. | Absent |
| Recommend refinement, adaption, termination, and execution of operational plans as appropriate. | Absent |
| Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities. | Absent |
| Submit or respond to requests for deconfliction of cyber operations. | Absent |
| Document lessons learned that convey the results of events and/or exercises. | Absent |
| Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement. | Absent |
| Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. | Absent |
| Provide expertise to course of action development. | Absent |
| Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials). | Absent |
| Contribute to crisis action planning for cyber operations. | Absent |
| Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers. | Absent |
| Coordinate with intelligence and cyber defense partners to obtain relevant essential information. | Absent |
| Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations. | Absent |
| Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives. | Absent |
| Develop strategy and processes for partner planning, operations, and capability development. | Absent |
| Develop, implement, and recommend changes to appropriate planning procedures and policies. | Absent |
| Develop, maintain, and assess cyber cooperation security agreements with external partners. | Absent |
| Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives. | Absent |
| Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community. | Absent |
| Identify and manage security cooperation priorities with external partners. | Absent |
| Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities. | Absent |
| Integrate cyber planning/targeting efforts with other organizations. | Absent |
| Maintain relationships with internal and external partners involved in cyber planning or related areas. | Absent |
| Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives. | Absent |
| Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy. | Absent |
| Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary. | Absent |
| Conduct long-range, strategic planning efforts with internal and external partners in cyber activities. | Absent |
| Provide subject matter expertise to planning efforts with internal and external cyber operations partners. | Absent |
| Propose policy which governs interactions with external coordination groups. | Absent |
| Prepare for and provide subject matter expertise to exercises. | Absent |
| Provide cyber focused guidance and advice on intelligence support plan inputs. | Absent |
| Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs. | Absent |
| Provide planning support between internal and external partners. | Absent |
| Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations. | Absent |
| Serve as a liaison with external partners. | Absent |
| Submit or respond to requests for deconfliction of cyber operations. | Absent |
| Synchronize cyber international engagement activities and associated resource requirements as appropriate. | Absent |
| Synchronize cyber portions of security cooperation plans. | Absent |
| Document lessons learned that convey the results of events and/or exercises. | Absent |
| Analyze internal operational architecture, tools, and procedures for ways to improve performance. | Present |
| Analyze target operational architecture for ways to gain access. | Present |
| Collaborate with development organizations to create and deploy the tools needed to achieve objectives. | Absent |
| Conduct access enabling of wireless computer and digital networks. | Present |
| Conduct collection and processing of wireless computer and digital networks. | Present |
| Conduct exploitation of wireless computer and digital networks. | Present |
| Conduct network scouting and vulnerability analyses of systems within a network. | Present |
| Conduct on-net activities to control and exfiltrate data from deployed technologies. | Present |
| Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies. | Present |
| Conduct open source data collection via various online tools. | Present |
| Conduct survey of computer and digital networks. | Present |
| Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers). | 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. | Present |
| Operate and maintain automated systems for gaining and maintaining access to target systems. | Absent |
| Conduct cyber activities to degrade/remove information resident in computers and computer networks. | Present |
| 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. | Present |
| Test internal developed tools and techniques against target tools. | Present |
| 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. | Present |
| Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals). | Present |
| Examine recovered data for information of relevance to the issue at hand. | Absent |
| Fuse computer network attack analyses with criminal and counterintelligence investigations and operations. | Absent |
| Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action. | Absent |
| Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations. | Absent |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. | Absent |
| Identify elements of proof of the crime. | Absent |
| Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations. | Absent |
| Process crime scenes. | Absent |
| Secure the electronic device or information source. | Absent |
| Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. | Absent |
| Analyze the crisis to ensure public, personal, and resource protection. | Absent |
| Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation. | Absent |
| Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks. | Absent |
| Provide criminal investigative support to trial counsel during the judicial process. | Absent |
| Analyze computer-generated threats for counter intelligence or criminal activity. | Absent |
| Gather and preserve evidence used on the prosecution of computer crimes. | Absent |
| Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes. | Absent |
| Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes. | Absent |
| Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking). | Absent |
| Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property. | Absent |
| Prepare reports to document the investigation following legal standards and requirements. | Absent |
| 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 |
| Analyze incident data for emerging trends. | Absent |
| Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. | Absent |
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. | Present |
| Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. | Present |
| Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data). | Absent |
| Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. | Absent |
| Analyze organizational cyber policy. | Present |
| Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion. | Present |
| Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis. | Present |
| 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. | Present |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. | Present |
| Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment. | Present |
| Perform file signature analysis. | Present |
| Perform hash comparison against established database. | Present |
| Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView). | Present |
| Perform timeline analysis. | Present |
| Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). | Absent |
| Perform static media analysis. | Present |
| Perform tier 1, 2, and 3 malware analysis. | Absent |
| Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures). | Absent |
| Provide technical assistance on digital evidence matters to appropriate personnel. | Absent |
| Recognize and accurately report forensic artifacts indicative of a particular operating system. | Absent |
| Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost). | Absent |
| Capture and analyze network traffic associated with malicious activities using network monitoring tools. | Absent |
| Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. | Absent |
| Conduct cursory binary analysis. | Absent |
| Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. | Absent |
| Perform virus scanning on digital media. | Absent |
| Perform file system forensic analysis. | Absent |
| Perform static analysis to mount an "image" of a drive (without necessarily having the original drive). | Absent |
| Perform static malware analysis. | Absent |
| Utilize deployable forensics toolkit to support operations as necessary. | Absent |
| Coordinate with intelligence analysts to correlate threat assessment data. | 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 defense reporting. | Absent |
| Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission. | Absent |
| Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. | Present |
| Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information. | Present |
| Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies. | Present |

**List of potential threats to Larsen and Toubro - LTI that could exploit vulnerabilities of critical assets due to missing Cybersecurity Specialty Areas, Cybersecurity Work Roles, and Cybersecurity Tasks**

|  |
| --- |
| **Threats** |
| Confidentiality and Privacy issues |
| Integrity issues |
| Availability issues |
| Authentication issues |
| Access Control issues |
| Non-Repudiation issues |
| Loss or Harm to Assets |

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

|  |
| --- |
| **Risks** |
| Increased number of technical errors |
| No proper guidance of testing the security softwares |
| Improper management of data |
| Lack of system security |
| No proper training to employees on cyber practices |
| Improper access control |
| No detailed check of individual systems and lacks analysis |
| Improper management during times of cyber attacks |
| No threat analysis could lead to higher chances of losses |
| No proper defense mechanisms against any attack or disrupting event |
| No guidance on how to investigate an event |
| Lack of Innovation |
| Limited Competitive Advantage |
| Inefficient Processes |
| Missed Opportunities |
| Lack of Future Vision |
| Quality issues |
| Legal liabilities |
| Increased costs |
| Inability to leverage data for business insights |
| Data quality issues |
| Poor system performance |
| Inadequate IT support at times of high need to customers |
| Poorly designed systems |
| Damage to company reputation |
| Lack of Security Awareness |
| Insider Threats |
| Malware Infections |
| Data Loss |
| Incomplete risk assessment |
| Delayed response to emerging threats |
| Limited situational awareness |
| Increased liability |
| Cash flow problems |
| Strained customer relationships |
| Increased bad debt |
| Lack of response capability |

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

* Larsen and Toubro - LTI should have an incident response plan in place that outlines the steps to take in the event of a cybersecurity incident. The plan should include a clear process for reporting incidents, assessing the damage, containing the threat, and restoring systems and data. All employees should be aware of this plan and trained on the procedures to follow.
* Larsen and Toubro - LTI can outsource cybersecurity services to a third-party vendor who specializes in cybersecurity. These vendors can provide incident response services, including forensics investigation, incident containment, and recovery.
* Regular security assessments can identify potential vulnerabilities and help prevent cyber attacks. The assessments can be conducted internally or by third-party vendors. Regular assessments can help identify weaknesses in the company's cybersecurity posture and enable proactive measures to mitigate the risk.
* In the absence of an INV department, the company should establish a response team that includes representatives from different departments, including IT, legal, and management. The response team should be trained and equipped to respond to incidents and coordinate with external experts, such as cybersecurity vendors, law enforcement agencies, and forensic investigators.
* Create a cybersecurity committee consisting of IT personnel, senior management, and representatives from different departments of the organization to oversee the organization's cybersecurity strategy.
* Conduct regular risk assessments to identify potential vulnerabilities and threats to the organization's network and data. This can be done using automated tools or through manual assessments.
* Develop a comprehensive cybersecurity plan that includes policies, procedures, and guidelines for protecting the organization's network and data.
* Establish Clear Payment Terms: The first policy to mitigate risks is to establish clear payment terms for all customers. This includes defining the payment schedule, late payment penalties, and the consequences of defaulting on payments. By having clear payment terms, customers will understand their responsibilities and the consequences of not meeting them.
* Conducting regular credit checks on customers is another policy that can help mitigate risks. This will help identify customers with a history of late payments or defaulting on debts. By doing so, Larsen and Toubro - LTI can take necessary precautions before providing credit or extending payment terms to these customers.
* Larsen and Toubro - LTI without a dedicated CLO department should create a delinquency management plan that outlines how overdue accounts will be managed. This plan should include steps for notifying customers of overdue payments, setting up payment plans, and taking legal action if necessary.
* Assigning responsibility for collections to specific individuals or departments is essential to ensure that overdue accounts are managed effectively. This includes establishing clear roles and responsibilities, providing necessary training and resources, and setting performance targets and KPIs.
* Larsen and Toubro - LTI should regularly monitor and review their collections performance to identify areas for improvement. This includes tracking key metrics such as days sales outstanding (DSO) and bad debt percentage, and making necessary changes to policies and procedures to improve performance.
* Larsen and Toubro - LTI can also leverage technology and automation to improve their collections processes. This includes using software tools to automate collections tasks such as sending reminders and managing payment plans, and using data analytics to identify trends and insights that can inform collections strategies.
* Create a centralized function responsible for collecting and analyzing intelligence from various sources, such as internal data, open-source intelligence, and industry reports. This function should work closely with business units and senior management to identify emerging risks and provide recommendations for mitigation.
* Invest in technology that can help automate the collection and analysis of data, such as artificial intelligence, machine learning, and data analytics tools. These technologies can help identify patterns and trends that might be missed by manual analysis.
* Engage external consultants with expertise in risk management, cybersecurity, and intelligence analysis to provide guidance and support in areas where the company may lack expertise.
* Create a centralized function responsible for collecting and analyzing intelligence from various sources, such as internal data, open-source intelligence, and industry reports. This function should work closely with business units and senior management to identify emerging risks and provide recommendations for mitigation.
* If the company cannot afford to hire a full-time TWA team, they can outsource these services to a reputable security consulting firm. This firm can conduct regular threat assessments and provide recommendations for mitigating risks.
* Larsen and Toubro - LTI should implement a security framework such as ISO 27001 or NIST Cybersecurity Framework to ensure that security controls are in place to protect against cyber threats. This framework should cover all aspects of the organization's operations, including people, processes, and technology.
* If Larsen and Toubro - LTI cannot afford to hire a full-time CDA team, it can hire a third-party security provider to provide security assessments, penetration testing, and other security services.
* Larsen and Toubro - LTI should regularly update software and systems to ensure that they are protected against known vulnerabilities. This includes implementing patches, upgrading to the latest versions of software, and regularly scanning systems for vulnerabilities.
* If Larsen and Toubro - LTI does not have the resources to create an EXL department, it can consider outsourcing cybersecurity to a third-party provider. The provider can be responsible for managing and mitigating cyber risks.

**PART C: Security Risk Management Recommendations**

**Security Risk Management Recommendations: Provide the list of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits based on your risk management analysis**

**For HGA:**

1. The highest ranked vulnerability is “False Time and Attendance Data sheets.” To solve that, Larsen and Toubro – LTI can:

* Establish clear policies and procedures for time and attendance tracking that all employees are aware of and trained on. This can include policies for clocking in and out, tracking sick days, and vacation time.
* Use automated time and attendance systems such as biometric systems, mobile apps or web-based tools can reduce the likelihood of false data and human error.
* Investigate the source of the false data by reviewing the time and attendance system and speaking with the employees involved.

1. The next highest is “Unknown Modifications/Destruction of Payroll Data.” To solve that, Larsen and Toubro – LTI can:

* Limit access to payroll data only to authorized personnel with a legitimate business need to access it. Implement strict password policies, and ensure that employees are trained on secure password management practices.
* Ensure that different employees are responsible for different aspects of payroll processing, such as data entry, approvals, and processing, to reduce the risk of fraud.
* Conduct a forensic analysis of the affected systems to determine the cause of the breach or data loss, and to identify any other compromised data or systems.

1. The third highest is, “Outdated software (lack of assurance due to improper authentication and encryption systems).” To solve that, Larsen and Toubro – LTI can:

* Implement a software update policy that requires regular updates to ensure software is up-to-date with the latest security patches and features.
* Ensure software is developed using secure coding practices that include authentication and encryption features.
* Conduct a thorough investigation to identify the root cause of the failure or breach.
* Communicate the incident to stakeholders and customers to ensure transparency.

1. The fourth is “Information disclosure.” To solve that, Larsen and Toubro – LTI can:

* Vet third-party vendors and contractors to ensure they have adequate security controls in place to protect sensitive information.
* Implement corrective measures to address any vulnerabilities or weaknesses that contributed to the information disclosure incident. This may include updating security controls, implementing additional monitoring, or improving employee training.
* Regularly back up all critical data to ensure that it can be recovered in the event of an information disclosure incident.

1. The last is “Relay Points (microwave stations/satellites).” To solve that, Larsen and Toubro – LTI can:

* Implement physical security measures such as surveillance cameras, access controls, and intrusion detection systems to prevent unauthorized access to the relay points. Also, implement cybersecurity measures such as firewalls, intrusion prevention systems, and regular vulnerability scanning to protect against cyber threats.
* Conduct regular maintenance and testing of relay points to ensure their proper functioning. This includes checking the equipment and verifying the signal strength and quality.
* Have trained technicians available to troubleshoot and diagnose issues with relay points quickly and effectively.

**For Larsen and Toubro – LTI, for every Risk, the following are the Preventive and Response measures to be implemented:**

1. Increased number of technical errors:

Regular system maintenance and updates

Automation of processes to reduce manual errors

Standardization of software and hardware configurations

Implementing quality assurance measures and testing protocols

1. No proper guidance of testing the security software:

Providing clear guidelines and procedures for testing security software

Regular training and education on security testing techniques

Third-party testing and validation of security software

1. Improper management of data:

Implementing data governance policies and procedures

Regular data backups and disaster recovery plans

Implementing access controls and permissions for data management

Monitoring and auditing of data access and usage

1. Lack of system security:

Implementing firewalls, intrusion detection and prevention systems, and antivirus software Regular security assessments and vulnerability scans

Penetration testing to identify system weaknesses

Continuous monitoring and logging of system activity

1. No proper training to employees on cyber practices:

Regular cybersecurity awareness training for all employees

Specific training for IT and security personnel

Security policies and procedures communicated to all employees

Regular reminders and updates on cybersecurity best practices

1. Improper access control:

Implementing access control policies and procedures

Two-factor authentication for sensitive data and systems

Regular review and audit of access permissions

Limiting access to critical systems and data

1. No detailed check of individual systems and lacks analysis:

Implementing a comprehensive inventory of systems and devices

Regular system assessments and audits

Analysis of system logs and activity

Patch management and updates to address vulnerabilities

1. Improper management during times of cyber attacks:

Incident response plan with defined roles and responsibilities

Regular incident response training and exercises

Rapid response and containment of incidents

Post-incident analysis and improvements to the incident response plan

1. No threat analysis could lead to higher chances of losses:

Regular threat assessments and analysis

Implementing a threat intelligence program

Proactive monitoring of emerging threats

Regular updates to security policies and procedures

1. No proper defense mechanisms against any attack or disrupting event:

Implementing disaster recovery and business continuity plans

Backup systems and data

Implementing redundancy for critical systems and services

Proactive monitoring for signs of attacks or disruptions

1. No guidance on how to investigate an event:

Incident response plan with defined investigation procedures

Forensic analysis tools and techniques

Training and education on incident investigation

Collaboration with law enforcement and other organizations if necessary

1. Lack of Innovation:

Encouraging innovation culture within the organization

Investing in research and development

Partnering with external innovation organizations

Regular reviews and updates to the innovation strategy

1. Limited Competitive Advantage:

Conducting regular market analysis and competitor research

Identifying unique selling points and value propositions

Investing in customer experience and service

Regular reviews and updates to the competitive strategy

1. Inefficient Processes:

Conducting regular process reviews and improvements

Implementing process automation and optimization

Regular training and education on process improvements

Identifying and addressing bottlenecks and inefficiencies

1. Missed Opportunities:

Conducting regular opportunity assessments and analysis

Identifying and prioritizing opportunities based on strategic goals

Rapid response to emerging opportunities

Regular reviews and updates to the opportunity strategy

1. Lack of Future Vision:

Developing a long-term strategic vision for the organization

Regular reviews and updates to the strategic plan

Investing in research and development for future products and services

Regular reviews of emerging technologies and trends

1. Quality issues:

Implementing quality assurance measures and testing protocols

Conducting regular quality control

1. Legal liabilities:

Regularly review and update policies and procedures to ensure compliance with relevant laws and regulations.

Conduct regular legal audits to identify and address potential legal risks.

Train employees on legal compliance and the importance of following policies and procedures.

1. Increased costs:

Implement cost-control measures, such as streamlining processes and reducing waste. Regularly review and optimize vendor contracts and relationships.

Conduct regular financial audits to identify and address potential cost issues.

1. Inability to leverage data for business insights:

Implement a data governance program to ensure data quality and accuracy.

Establish a data management strategy that includes data integration, storage, and analytics. Ensure data security and privacy by implementing proper access controls and data encryption.

1. Data quality issues:

Implement data quality controls, such as data validation and cleansing.

Regularly review and audit data sources and processes to identify and address quality issues.

Train employees on data quality best practices.

1. Poor system performance:

Regularly monitor system performance and conduct performance testing to identify and address issues.

Implement system upgrades and enhancements to improve performance.

Train employees on system performance best practices.

1. Inadequate IT support at times of high need to customers:

Develop a comprehensive IT support plan that includes staffing, training, and escalation procedures.

Implement a self-service IT support portal for customers. Regularly review and optimize IT support processes and procedures.

1. Poorly designed systems:

Conduct regular system design reviews to identify and address design flaws.

Implement user-centered design principles to ensure systems meet user needs and expectations.

Ensure systems are built using secure coding practices.

1. Lack of Security Awareness:

Develop and implement a comprehensive security awareness program that includes training and education.

Conduct regular security audits to identify and address security weaknesses.

Regularly communicate security policies and procedures to employees and customers.

1. Insider Threats:

Implement access controls and monitoring to prevent unauthorized access to sensitive data.

Conduct regular employee background checks and monitor employee behavior for suspicious activity.

Train employees on security best practices and the importance of reporting suspicious activity.

1. Malware Infections:

Implement anti-malware software and keep it up-to-date.

Regularly scan systems for malware and suspicious activity.

Train employees on how to identify and avoid malware infections.

1. Data Loss:

Implement data backup and recovery processes to ensure data can be restored in the event of data loss.

Regularly test data backup and recovery processes to ensure they work as intended.

Train employees on data backup and recovery procedures.

1. Incomplete risk assessment:

Develop and implement a comprehensive risk assessment process that includes identifying, assessing, and prioritizing risks.

Regularly review and update risk assessments to ensure they are accurate and up-to-date. Involve stakeholders from across the organization in the risk assessment process.

1. Delayed response to emerging threats:

Develop and implement a comprehensive incident response plan that includes procedures for responding to emerging threats.

Regularly test incident response procedures to ensure they work as intended.

Train employees on incident response procedures.

1. Limited situational awareness:

Implement real-time monitoring and analytics tools to provide situational awareness. Conduct regular threat intelligence analysis to identify emerging threats.

Train employees on situational awareness best practices.

1. Increased liability:

Regularly review and update insurance policies to ensure adequate coverage.

Implement risk mitigation strategies to reduce liability exposure.

Train employees on liability risk management best practices

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

**For HGA:**

* Residual Risk with current controls: $1000000
* Residual Risk with new controls: $60000
* Proposed Security Risk Budget Cost: $680000

**Residual Risk Reduction:**

* Residual Risk with current controls - Residual Risk with new controls

= $1000000 - $60000

**=** $940000

This is greater than the proposed security risk budget

**Cost benefit ratio analysis for mixed/proposed budget**

= Proposed security risk budget / expected security risk benefit

= 680000 / 940000

= 0.723404

**For Larsen and Toubro – LTI:**

* Residual Risk with current controls: $1500000
* Residual Risk with new controls: $90000
* Proposed Security Risk Budget Cost: $880000

**Residual Risk Reduction:**

* Residual Risk with current controls - Residual Risk with new controls

= $1500000 - $90000

**=** $1410000

This is greater than the proposed security risk budget

**Cost benefit ratio analysis for mixed/proposed budget**

= Proposed security risk budget / expected security risk benefit

= 880000 / 1410000

= 0.624113

**Compare your proposed security controls, methods and policies budget for HGA (which is based on security risk assessment in Part A) with the proposed security controls, methods and policies budget for your company (which is based on security risk implementation plan in Part B), adjusting for industry, mission, scale, threat environment and workforce differences between HGA and your company.**

|  |  |  |
| --- | --- | --- |
| Point of Comparison | HGA | Larsen and Toubro - LTI |
| Type of Enterprise | Financial - Government | Private - IT services and consulting company |
| Mission | Deals with financial transfer to different government agencies | Offers application development, testing, maintenance, cloud, cognitive/ artificial intelligence and enterprise solutions |
| Geographic Presence | United States of America | Global Presence |
| Network Topology | Appendix 3 | Appendix 4 |
| Number Of Employees | 200 | 2000 |
| Clients | Government Agencies of USA | Enterprises belonging to Big Data Analytics, Business Process Automation, BlockChain, Artificial Intelligence, Robotic Process Automation domains |
| Critical Asset Value | $700,000 | $6,000,000 |
| Threat Environment | Nation State, Organizations, Hacker Organizations | Insider Environment, Nation State, Competitors, Investors |
| Threat Agents | Cyber attackers, Hacktivists, Cyber groups | Cyber groups, Insider threats, Hackers |
| Residual Security Risk in $ | $60000 | $90000 |
| Budget for Risk Prevention and Risk Response Controls, Methods and Policies | $680000 | $880000 |
| $ Security Budget / $Security Risk Improvement | 0.723404 | 0.624113 |
| $ Security Budget / $ Critical Assets | 0.971428 | 0.146666 |
| $ Security Budget / $ Employees | 3400 | 440 |

Attack Tree for Hypothetical Government Agency (HGA)

Disruption to the working of the organization

Financial Losses and Unexplainable Costs

Loss of Access Control

Data and Security Breach

Loss of Confidentiality

Relay Points

Information disclosure

Outdated software

Unknown Modifications/Destruction of Payroll Data

False Time and Attendance Data sheets

Cyber groups

Hacktivists

Cyber attackers

Attack Tree for Larsen and Toubro - LTI

Improper Services to Clients

Defects in Services

No guaranteed security

Lack of Availability

Difficulty in implementing software testing processes

Manual checking

Increased Man-in-the-middle attacks

Lack of port security

Hackers

Insider Threats

Cyber groups

**Vulnerabilities and Exploitation Probabilities**

**For HGA:**

|  |  |
| --- | --- |
| **Vulnerability** | **Exploitation Probability** |
| False Time and Attendance Data sheets | 95 |
| Unknown Modifications/Destruction of Payroll Data | 95 |
| Outdated software (lack of assurance due to improper authentication and encryption systems) | 90 |
| Information disclosure | 98 |
| Relay points (microwave stations/satellites) | 70 |
| Improper policies and regulations | 65 |
| Failing to comply with the established standards | 50 |

**For Larsen and Toubro – LTI:**

|  |  |
| --- | --- |
| **Vulnerability** | **Exploitation Probability** |
| Manual checking | 98 |
| Lack of system security | 60 |
| Sensitive information disclosure | 70 |
| Social Engineering | 89 |
| Increase Attack surface | 88 |
| Increase in Cyber attacks | 50 |
| Data interception | 50 |
| Unknown data modifications/stealing of data | 60 |
| Difficulty in monitoring user activity | 70 |
| SYN Attacks flooding | 80 |
| Ease of VLAN access | 90 |
| Lack of port security | 98 |
| Interruption in operations | 50 |
| Inconsistent access control | 70 |
| Theft | 70 |
| Higher risk of errors | 90 |
| Unknown data/file modifications | 30 |
| Limited traceability | 60 |
| Malware infection | 50 |
| System crashes | 60 |
| Difficulty in implementing software testing processes | 98 |
| Lower rate of performance | 70 |
| Does not adhere to compliance | 80 |
| Increased Man-in-the-middle attacks | 98 |
| Identity spoofing | 80 |
| Denial of Service attacks | 60 |
| Difficulty in identifying networks | 50 |
| Interference with other networks | 40 |
| Ease of unauthorized access | 70 |
| Ease of fooling the systems | 20 |

**Cybersecurity workforce recommendations:**

**For HGA:**

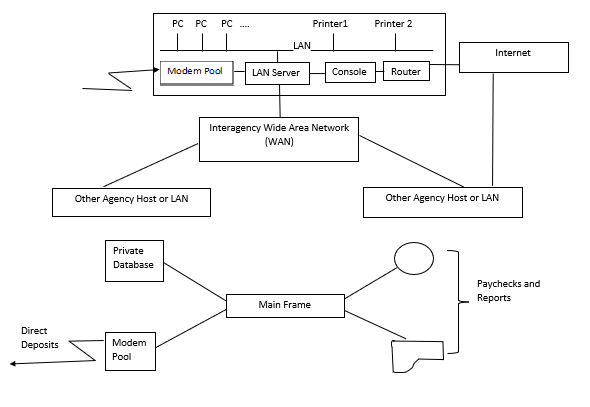
* Database and System Administrator should be trained
* Backup, Recovery and Maintenance controls need to be updated on a periodic basis
* It is important for HGA to implement the Industrial Controls of ISO 9001 and ISO 27001 to fulfill the compliance with applicable laws and regulations
* Adequate incident response management process should be implemented which will have an incident response team in place of any incident

**For Larsen and Toubro – LTI:**

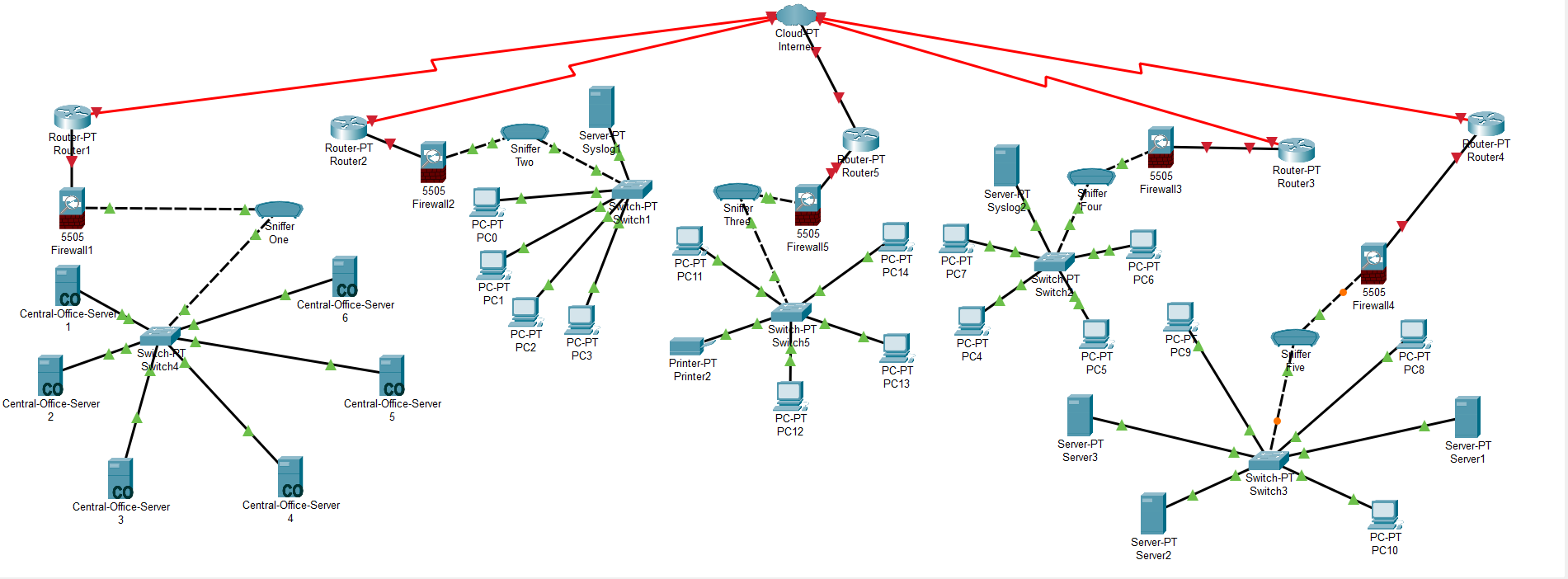
* Larsen and Toubro – LTI needs to have a continuous process to update their security policies for them to adhere to the governmental compliance
* Training and Educational Sessions on security principles need to be mandated
* Disaster Recovery and Business Continuity plans need to be laid from the very beginning to contain any upcoming risks and threats
* Cyber Security Operators should be in place to make sure that all regulations, laws and all other aspects of cyber security are being found.

**PART D: APPENDIX**

Appendix 3: Detailed Network Topology for HGA



Appendix 4: Detailed Network Topology(defense-in-depth) for Larsen and Toubro – LTI



The picture above depicts the simpler version of Larsen & Toubro Infotech -LTI’s organizational network. The company is engaged in application development, testing, maintenance and outsourcing, infrastructure management, digital solutions, and platform-based solutions. It offers solutions for domains such as Internet of things (IoT), cloud, cognitive/ artificial intelligence, enterprise solutions, Big Data Analytics, Business Process Automation, BlockChain, Artificial Intelligence, Robotic Process Automation, Machine Learning, GDPR Compliance, Digital Consulting, Information Technology, Cloud Migration, Digital Transformation, Data Analytics, and Privacy. Since it supports and provides various kinds of services, it is important to have isolated sub-networks.

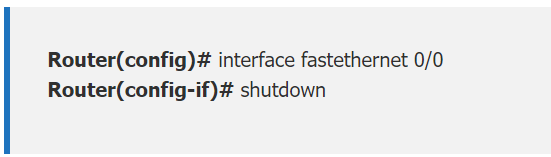
The different sub-networks seen are: Data center, Finance department, Software and Security Development department, Legal Advisory department and Customer Service and Technical Support department. The subnetworks maintain security controls of limiting the access and follow the legal compliance standards to secure all customer data. All departments have servers for storing data and these have automatic update systems that update data from the user devices periodically.

All departments data which is stored into individual servers are also stored into Central Servers as a copy to help retrieve data in crucial times. These Central Office Servers form separate subnetwork as the “Datacenter” and need high physical and logical level security.

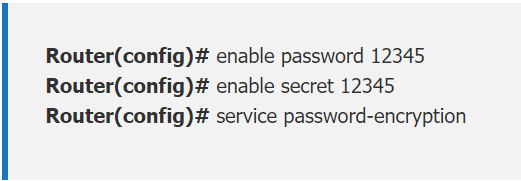
Each departmental subnetwork has User Work Stations (PC’s), Printers, Servers, Switches, Sniffers (which act like Test Access Points), ASA Firewalls and Routers. All subnetworks are connected to each other through the Internet. Routers act as entry gateways for every subnetwork. The traffic is then analyzed by the Firewall. Firewalls scan the entry requests to be genuine and only upon verification allow entry to the subnetwork. Sniffers on the next level monitor network traffic and performance. Switches upon receiving the request check for Link layer data and accordingly forwards the traffic to particular User Station only.

Updates to the network:

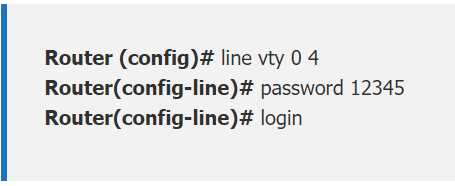
1. Disabling unused ports: The following CLI Commands can be configured on all Routers to disable unused ports which ensures more security



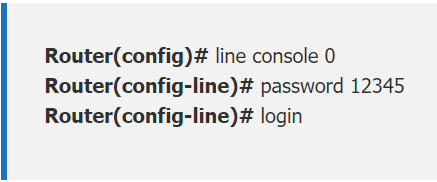
1. Enable complex passwords to Routers: This allows routers to be only accessible to authorized users



1. Configuring Telnet Access Password: Tenet is a secure way of connecting to a router and hence we enable telnet password



1. Configuring Console Access Password: Console access control can be managed by enabling console access passwords



**References:**

1. [https://www.aura.com/learn/fingerprint-identity-theft#:~:text=Using%20a%203D%20printer%20to,a%20police%20investigation%20%5B\*%5D](https://www.aura.com/learn/fingerprint-identity-theft#:~:text=Using%20a%203D%20printer%20to,a%20police%20investigation%20%5B*%5D).
2. <https://www.embroker.com/blog/cyber-incident-response-plan/#:~:text=A%20cyber%20incident%20response%20plan%20is%20a%20written%20set%20of,recover%20from%20a%20cyber%20attack>.
3. <https://www.techtarget.com/searchsecurity/answer/How-do-a-DMZ-and-VPN-work-together>
4. <https://www.sgcybersecurity.com/images/resource/SOPs/Network_Policy/remote_access_tools_policy.pdf>
5. <https://www.techtarget.com/searchsecurity/feature/The-five-different-types-of-firewalls>
6. <https://www.niatec.iri.isu.edu/(S(5pvzas455hrdzsrxbwh1ndqb))/GetFile.aspx?pid=606>
7. <https://www.sgcybersecurity.com/images/resource/SOPs/Network_Policy/router_and_switch_security_policy.pdf>
8. <https://blog.totalprosource.com/8-preventative-security-controls-you-should-consider>
9. <https://www.ibm.com/topics/security-controls#:~:text=Digital%20security%20controls%20include%20such,mitigation%2C%20and%20intrusion%20prevention%20systems>.
10. <https://www.cybersaint.io/blog/8-nist-security-controls-to-focus-on-during-and-after-a-crisis>
11. <https://www.ibm.com/docs/en/i/7.3?topic=security-ip-filtering-network-address-translation>
12. <https://www.csirt.org/sample_policies/sans/Virtual_Private_Network.doc>
13. <https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt0a307ae2bb5b3b62/5e9dfa093acb0660063feb59/remote_access_tools_policy.pdf>
14. <https://www.beyondtrust.com/resources/glossary/privileged-access-management-pam#:~:text=Privileges%20serve%20an%20important%20operational,and%20complete%20work%2Drelated%20tasks>.
15. <https://jwcn-eurasipjournals.springeropen.com/articles/10.1186/1687-1499-2011-101>
16. <https://www.edq.com/blog/3-ways-to-prepare-your-data-for-the-unknown/>
17. <https://content.dsp.co.uk/the-key-responsibilities-of-a-database-administrator>
18. <https://sobekdigital.com/securitypolicies/database_credentials_policy.pdf>
19. <https://blog.totalprosource.com/8-preventative-security-controls-you-should-consider>
20. <https://www.ibm.com/topics/security-controls#:~:text=Digital%20security%20controls%20include%20such,mitigation%2C%20and%20intrusion%20prevention%20systems>.
21. <https://www.cybersaint.io/blog/8-nist-security-controls-to-focus-on-during-and-after-a-crisis>
22. <https://www.ibm.com/docs/en/i/7.3?topic=security-ip-filtering-network-address-translation>
23. <https://assets.contentstack.io/v3/assets/blt36c2e63521272fdc/blt836d5fac43a8727f/5e9dfd035661cd12411d53a6/wireless_communication_standard.pdf>
24. <https://www.sgcybersecurity.com/images/resource/SOPs/Network_Policy/wireless_communication_policy.pdf>