Graphical user interface

Description automatically generated with low confidence

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

Instructor: Professor Themis A. Papageorge

Student Name: Varunsai Valluripalli

NUID: 002929218

**Table of Contents**

|  |  |  |
| --- | --- | --- |
| **Part** | **Title** | **Page Number** |
|  |  |  |
| **Part A** | **Security Risk Management Assessment** | 5-39 |
|  | Executive Summary | 5-8 |
|  | List of Assets with Values ($) | 9 |
|  | List of Threats | 9-10 |
|  | List of Vulnerabilities | 10 |
|  | Threat/Vulnerability pairs | 10-11 |
|  | Assets impacted by Threat/vulnerability Pairs | 11-12 |
|  | MOT-which MOT controls are covered by current HGA controls | 13-15 |
|  | MOT- proposed by new CISO HGA controls and a VPN server and DMZ | 15-17 |
|  | Security Risk Prevention Strategy | 17-25 |
|  | Security Risk Response Strategy | 25-34 |
|  | Mixed Security Risk Prevention Strategy and Security Risk Response Strategy | 34-37 |
|  | Conclusion: Cost-Benefit Analysis | 37-39 |
|  |  |  |
| **Part B** | **Security Risk Management Implementation Plan** | 41-161 |
|  | Access Control Security Risk Management Implementation Controls and Policies | 41-42 |
|  | Network Infrastructure Security Risk Management Implementation Controls and Policies | 42-43 |
|  | Network Infrastructure Management Security Risk Management Implementation Controls and Policies | 44-45 |
|  | Database Security Risk Management Implementation Controls and Policies | 45-47 |
|  | Applications Development Security Risk Management Implementation Controls and Policies | 48-49 |
|  | Wireless Security Risk Management Implementation Controls and Policies | 49-50 |
|  | List of Cybersecurity Implementation Controls at Kshemin Innovations PVT LTD | 51-56 |
|  | Comparison of the Implementation controls discusses in class with Kshemin Innovations PVT LTD’s existing Cybersecurity Implementation controls | 57-64 |
|  | List of critical assets that exist in Kshemin Innovations PVT LTD | 64 |
|  | List of Potential Vulnerabilities at Kshemin Innovations PVT LTD | 64 |
|  | List of Potential Threats at Kshemin Innovations PVT LTD | 65 |
|  | List of Potential Risks at Kshemin Innovations PVT LTD | 65 |
|  | List of recommended Hardening Prevention controls and policies | 66 |
|  | List of recommended Hardening Response controls and policies for critical assets | 67 |
|  | Applicable Government Regulations and Industry Standards | 67 |
|  | Rank asset risks and vulnerability risks | 68-69 |
|  | List of Cybersecurity Specialty Areas that exist in Kshemin Innovations PVT LTD | 71-72 |
|  | List of Cybersecurity Work roles that exist in Kshemin Innovations PVT LTD | 72 |
|  | List of Cybersecurity Tasks that exist in Kshemin Innovations PVT LTD | 72-75 |
|  | Comparison of the NCWF recommended Cybersecurity Specialty Areas with Kshemin Innovations PVT LTD’s existing Cybersecurity Specialty Areas | 75-76 |
|  | Comparison of the NCWF recommended Cybersecurity Work Roles with Kshemin Innovations PVT LTD’s existing Cybersecurity Work Roles | 76-159 |
|  | Comparison of the NCWF recommended Cybersecurity Tasks with Kshemin Innovations PVT LTD’s existing Cybersecurity Tasks | 76-159 |
|  | List of Potential threats to Kshemin Innovations PVT LTD | 159 |
|  | List of potential risks for Kshemin Innovations PVT LTD | 160 |
|  | List of recommended policies that should be created to mitigate the identified risks | 160-161 |
|  |  |  |
| **Part C** | **Security Risk Management Recommendations** | 163-170 |
|  | List of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits | 163-164 |
|  | Provide the total cost and benefit in $  Compare your proposed security controls, methods, and policies budget for HGA with the proposed security controls, methods, and policies budget for Kshemin Innovations PVT LTD | 165-166 |
|  | Attack Tree for HGA | 167 |
|  | Attack Tree for Kshemin Innovations PVT LTD | 168 |
|  | Vulnerabilities and Exploitation Probabilities | 169 |
|  | Cybersecurity Workforce Recommendations | 170 |
|  |  |  |
| **Part D** | **Appendix** | 172-175 |
|  | Appendix 3: Detailed Network Topology for HGA | 172 |
|  | Appendix 4: Detailed Network Topology for Kshemin Innovations PVT LTD | 173 |
|  | References | 174-175 |

**PART A: SECURITY RISK MANAGEMENT ASSESSMENT**

**Executive Summary**

**Information System Name:** Hypothetical Government Strategy

**Information System Categorization**:

|  |  |  |  |
| --- | --- | --- | --- |
| **Assets** | **Information Security Elements** | | |
|  | **Confidentiality(C)** | **Integrity(I)** | **Availability(A)** |
| Hard Disk | Medium | Medium | Medium |
| Personnel Information | High | High | High |
| Console | High | High | High |
| WAN or LAN Router | Medium | Medium | Medium |
| VPN Server | High | High | High |
| A screened subnet with DMZ | High | High | High |
| LAN Server | High | High | High |

**Organization Name**: Hypothetical Government Agency

**Organization Address**: 1131 Commonwealth Avenue, Boston, 02134

Asish Veerni

**Title**: Chief Executive Officer

**Email**: veerni27@gmail.com

**Phone**: +1 6784561234

Ravikiran Tulasi

**Title**: Chief Information Officer

**Email**: ravikiran2@gmail.com

**Phone**: +1 6432745821

Chandra Mouli Somisetty

**Title**: Chief Financial Officer

**Email**: moulichandra@gmail.com

**Phone**: +1 8754213489

Siva Manikanta Rangana

**Title**: Chief Information Security Officer

**Email**: Manikantar@gmail.com

**Phone**: +1 7459864322

**Information System Operation Status**: Operational

**Information System Type**: Major Application

**System Description**: Funds transfer to individual consumers and budget allocation to various departments from the US Government

**System Environment**: Please refer appendix 3

**Interconnection of System Information:**

**System Name**: Government Agency

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

**Type of Agreement**: Government Contract

**Date**: March 13, 1994

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

**C&A Category**: Accredited and Certified

**Authorizing Official**: Ravikiran Tulasi

**List of applicable laws/frameworks/standards/policies/regulations**:

* American National Standards Institute (ANSI)
* Federal Information Security Management Act (FISMA) of 2002
* National Institute of Standards and Technology (NIST)
* ISO/IEC 7810
* The Privacy Act
* Computer Security Act of 1987
* Sarbanes Oxley Act of 2002
* Federal Acquisition Regulation System
* Gramm-Leach-Bliley Act of 1999

**Minimum Security Controls**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Security Control | Observations | Status | Content-Type | Responsible Authority |
| Policies – M1 | Policies framed by the government are being followed | Complete | Common | CISO |
| Life Cycle Planning – M2 | Short-term goals are kept in mind as of time being | Partial | Common | CIO |
| Program Management – M3 | Main aim of the entire agency is kept in mind always | Complete | Common | CIO |
| Risk Management – M4 | Estimation and solving the possible threats will always be in action | Partial | Common | CISO |
| Personnel/User Issues – M5 | User issues need to be checked into in a more detailed way | Partial | Common | CIO |
| Incident Reporting and Handling – M6 | Where and how to report in case of a threat incident is taught in a detailed way | Complete | Common | CISO |
| Awareness, Training, and Education – M7 | Training of all methods and procedures is done completely | Complete | Common | CIO |
| Physical and Environmental Security – M8 | The network and system security should be done more deeply | Partial | Common | CISO |
| Contingency planning – M9 | Proper future planning should be done with a long future in mind | Partial | Common | CIO |
| Documentation – M10 | Proper documentation of every incident is being done | Complete | Common | CIO |
| Hardware and software system maintenance – M11 | Regular maintenance of hardware and software is being done | Complete | Common | CISO |
| Identification and Authentication – M12 | Authentication is done properly | Complete | Common | CISO |
| Login Access Control – M13 | Logins are verified clearly | Complete | Common | CISO |
| Cryptography – M14 | Advanced cryptographic algorithms are in place | Complete | Common | CISO |
| Audit Trails – M15 | Auditing and checking must be made stricter | Partial | Common | CISO |

Information Security Plan complete date: 2/12/2022

Information Security Plan Approval date: 2/19/2022

Considering a hypothetical government agency consisting of 175 employees and 225 computers to work with. It has many assets as stated below:

Hard disks = 125 \* $150 = $18750

LAN Server = $40000

Personal Information = 175 \* $1000 = $175000

Console = 10 \* $800 = $8000

Business Documents = $200000

WAN or LAN Router = 250 \* $200 = $50000

Printers = 200 \* $150 = $30000

**Assets**:

|  |  |  |  |
| --- | --- | --- | --- |
| Asset Number | Asset Name | Asset Description | Value |
| A1 | LAN Server | A powerful computer used for storage and for sharing information to other devices | $40000 |
| A2 | Hard Disk | Memory storage device | $18750 |
| A3 | Personnel Information | User details such as passwords, mobile numbers, address | $175000 |
| A4 | Console | It is like an application software that is provided to monitor and configure data. | $8000 |
| A5 | Business Documents | Documents involving information about financial dealings | $200000 |
| A6 | Email | Emails containing valuable information about companies | $100000 |
| A7 | WAN or LAN Router | Used to connect and send packets of data to multiple networks | $50000 |
| A8 | Printer | Used to print important documents | $30000 |
| A9 | Draft Rules | Gives rules and regulations of what needs to be followed in an institution | $10000 |
| A10 | VPN Server | Helps to extend a private network across a public network | $3000 |
| A11 | A screened subnet with DMZ | Helps in increasing network security | $30000 |

**Threats**:

|  |  |
| --- | --- |
| Threat Number | Threat |
| T1 | Financial Fraud |
| T2 | Errors in data entry |
| T3 | Interruption of Operations |
| T4 | Malicious Employee |
| T5 | Exposing crucial information |
| T6 | Network-based problems |
| T7 | Threats caused by insufficient space to store data |

**Vulnerabilities**:

|  |  |
| --- | --- |
| Vulnerability number | Vulnerability |
| V1 | Improper storage of time and attendance information |
| V2 | Usage of relay points by WAN service provider |
| V3 | Including other accessible files in the email utility |
| V4 | Not running a virus scanner |
| V5 | Improper backup of information in storage devices |
| V6 | Unauthorized Access |
| V7 | Improper data modification applications in the server |
| V8 | Password-based management for a mainframe |

**Asset/Vulnerability pairs**:

|  |  |
| --- | --- |
| Asset | Vulnerability |
| A1 | V4: Not running a virus scanner |
| V5: Improper backup of information in storage devices |
| V6: Unauthorized Access |
| A3 | V4: Not running a virus scanner |
| V6: Unauthorized Access |
| V2: Usage of relay points by WAN service provider |
| A2 | V5: Improper backup of information in storage devices |
| A4 | V2: Usage of relay points by WAN service provider |
| V6: Unauthorized Access |

**Threat-Vulnerability pairs for Assets in the HGA case study**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 |
| T1 | 78 | 86 | 73 | 94 |
| T2 | 41 | 53 | 93 | 78 |
| T4 | 83 | 70 | 51 | 87 |
| T6 | 92 | 59 | 57 | 63 |

**Current Security Controls and Policies**:

|  |  |  |
| --- | --- | --- |
| Number | Name | Description |
| 1. | Appendix III to OMB circular number A-130 | Controls for automated information security |
| 2. | The Computer Security Act of 1987 | Intended to protect sensitive information in federal computer systems |
| 3. | The Privacy Act | Submitting system records to the federal register |
| 4. | OMB Circular A-123 | It defines management responsibilities for internal controls |
| 5. | OMB Circular A-127 | It frames standards regarding financial data |
| 6. | Federal Manager’s Financial Integrity Act | To maintain internal control to reach the objectives |

**New Security Controls and policies with MOT Controls**:

|  |  |  |  |
| --- | --- | --- | --- |
| Number | Name | Description | MOT Controls |
| 1 | Policy on control and operation of system components | Modification and usage should only be done by HGA | M1, M4, M8, M11, M12, M13, M14, M15 |
| 2 | Issue-specific policy on the Internet | Use of e-mail with outside organizations and access to other resources. | M4, M8, M11, M12, M13, M15 |
| 3 | Need-To-Know-Policy | Information should be accessible only to HGA employees. | M1, M3, M4, M7, M12, M13 |
| 4 | Policy on storing and retrieving information | Proper storage of files in hard disks | M1, M3, M4, M7, M8, M10, M12, M13, M15 |
| 5 | Virus protection policy | Downloading various anti-virus for protection | M1, M4, M7, M8, M11, M15 |
| 6 | Policy for implementing advanced methods for authentication | To ensure trusted access to the systems of HGA | M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, M12, M13, M14, M15 |

**Subset of Assets**:

|  |  |  |  |
| --- | --- | --- | --- |
| Asset number | Asset name | Asset description | Value assigned |
| A1 | LAN server | A powerful computer used for storage and for sharing information to other devices | $40000 |
| A3 | Personnel Information | User details such as passwords, mobile numbers, address | $175000 |
| A2 | Hard Disk | Memory storage device | $18750 |
| A4 | Console | It is like an application software that is provided to monitor and configure data. | $8000 |

**Subset of Threats**:

|  |  |
| --- | --- |
| Threat number | Threat |
| T1 | Financial Fraud |
| T2 | Errors in data entry |
| T4 | Malicious Employee |
| T6 | Network-based problems |

**Subset of Vulnerabilities**:

|  |  |
| --- | --- |
| Vulnerability number | Vulnerability |
| V2 | Usage of relay points by WAN service provider |
| V4 | Not running a virus scanner |
| V5 | Improper backup of information in storage devices |
| V6 | Unauthorized Access |

**Threat-Vulnerability pairs**:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 |
| T1 | 78 | 86 | 73 | 94 |
| T2 | 41 | 53 | 93 | 78 |
| T4 | 83 | 70 | 51 | 87 |
| T6 | 92 | 59 | 57 | 63 |

Total Threat = 1158

The explanation for the assigned values:

* In the case of T1 which is financial fraud, it can be considered as a serious threat because information dealing with money is sensitive, and if it is altered or falls into malicious people, the reputation of a company can be lost. So, unauthorized access gives control of important documents to outsiders who can make use of them negatively and that is why it is given the highest probability.
* In the case of T2 which is errors in data entry, mistakes in the information can cause serious effects to an institution in the long way run. Improper storage of data can be harmful because in some situations data need to be retrieved, and if the whole data is not collected back, it leads to the false calculation of data. Hence, improper storage is given the highest probability.
* When a malicious employee working within the organization gets control of files that he is not supposed to get accessed with, he might expose the information to the wrong people. Hence, unauthorized access is given more chance for this threat.
* Network-based threats are dangerous. Many people can get access at some points in a vast network. If a WAN service provider uses a relay point in between to transfer data everywhere, those relay points can act as data spilling points, and hence it is given more probability.

**Asset/Vulnerability pairs**:

|  |  |
| --- | --- |
| Asset | Vulnerability |
| A1 | V4: Not running a virus scanner |
| V5: Improper backup of information in storage devices |
| V6: Unauthorized Access |
| A3 | V4: Not running a virus scanner |
| V6: Unauthorized Access |
| V2: Usage of relay points by WAN service provider |
| A2 | V5: Improper backup of information in storage devices |
| A4 | V2: Usage of relay points by WAN service provider |
| V6: Unauthorized Access |

**MOT Controls**:

|  |  |  |
| --- | --- | --- |
| Management | Operational | Technical |
| Policies – M1 | Personnel/User Issues – M5 | Identification and Authentication – M12 |
| Life Cycle Planning – M2 | Incident Reporting and Handling – M6 | Login Access Control – M13 |
| Program Management – M3 | Awareness, Training, and Education – M7 | Cryptography – M14 |
| Risk Management – M4 | Physical and Environmental Security – M8 | Audit Trails – M15 |
|  | Contingency planning – M9 |  |
|  | Documentation – M10 |  |
|  | Hardware and software system maintenance – M11 |  |

**Current Security Controls and Policies with MOT Controls**:

|  |  |  |  |
| --- | --- | --- | --- |
| Number | Name | Description | Management-Operational-Technical Controls |
| 1. | Appendix III to OMB circular number A-130 | Controls for automated information security | M1, M2, M4, M8, M12, M14 |
| 2. | The Computer Security Act of 1987 | Intended to protect sensitive information in federal computer systems | M4, M5, M6, M9, M11, M12, M14 |
| 3. | The Privacy Act | Submitting system records to the federal register | M1, M3, M4, M6, M7, M9, M10 |
| 4. | OMB Circular A-123 | It defines management responsibilities for internal controls | M1, M2, M3, M4, M9, M10, M13, M15 |
| 5. | OMB Circular A-127 | It frames standards regarding financial data | M1, M3, M5, M11, M15, M12, M14, M13 |
| 6. | Federal Manager’s Financial Integrity Act | To maintain internal control to reach the objectives | M3, M6, M7, M9, M15 |

**New Security Controls and policies with MOT Controls**:

|  |  |  |  |
| --- | --- | --- | --- |
| Number | Name | Description | MOT Controls |
| 1 | Policy on control and operation of system components | Modification and usage should only be done by HGA | M1, M4, M8, M11, M12, M13, M14, M15 |
| 2 | Issue-specific policy on the Internet | Use of e-mail with outside organizations and access to other resources. | M4, M8, M11, M12, M13, M15 |
| 3 | Need-To-Know-Policy | Information should be accessible only to HGA employees. | M1, M3, M4, M7, M12, M13 |
| 4 | Policy on storing and retrieving information | Proper storage of files in hard disks | M1, M3, M4, M7, M8, M10, M12, M13, M15 |
| 5 | Virus protection policy | Downloading various anti-virus for protection | M1, M4, M7, M8, M11, M15 |
| 6 | Policy for implementing advanced methods for authentication | To ensure trusted access to the systems of HGA | M1, M2, M3, M4, M5, M6, M7, M8, M9, M10, M11, M12, M13, M14, M15 |

**Security Risk Prevention Strategy**

**Initial Risk Impact:** Considering System Resilience as 0

Threat-Vulnerability Pair for the subset of Assets A1, A3, A2, A4:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 | V8 |
| T1 | 14 | 17 | 14 | 16 | 18 |
| T2 | 15 | 15 | 19 | 20 | 19 |
| T4 | 16 | 14 | 15 | 15 | 12 |
| T6 | 18 | 13 | 17 | 17 | 19 |
| T5 | 19 | 12 | 13 | 11 | 15 |

**Risk Impact Matrix**:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1V2 | T1V4 | T1V5 | T1V6 | T1V8 | T2V2 | T2V4 | T2V5 | T2V6 | T2V8 | T4V2 | T4V4 | T4V5 | T4V6 | T4V8 | T6V2 | T6V4 | T6V5 | T6V6 | T6V8 | T5V2 | T5V4 | | T5V5 | | T5V6 | | T5V8 | |
| A1 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 55 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | | 100 | | 100 | |
| A3 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | | 100 | | 100 | |
| A2 | 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 | |
| A4 | 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 | |
| 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 | |
| A11 | 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 | |

**Calculating Residual Asset Security Risk**:

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Asset Value | Total Threat | Residual Asset Security Risk = (Asset\*Total Threat) /100 |
| A1 | $40000 | 393 | $157200 |
| A3 | $175000 | 393 | $687750 |
| A2 | $18750 | 393 | $73687 |
| A4 | $8000 | 393 | $31440 |
| A10 | $3000 | 393 | $11790 |
| A11 | $30000 | 393 | $117900 |

**Calculating Residual Vulnerability Security Risk**:

Risk due to V2: [(A1\*total V2 = $40000\*82) +(A3\*total V2 = $175000\*82) +(A2\*total V2 = $18750\*82) +(A4\*total V2 = $8000\*82) +(A10\*total V2 = $3000\*82) +(A11\*total V2 = $30000\*82)] / 100 = $224495 < $274750

Risk due to V4: [(A1\*total V4 = $40000\*71) +( A3\*total V4 = $175000\*71) +( A2\*total V4 = $18750\*71) +(A4\*total V4 = $8000\*71) +(A10\*total V2 = $3000\*71) +(A11\*total V2 = $30000\*71)] / 100 = $195072 < $274750

Risk due to V5: [(A1\*total V5 = $40000\*78) +( A3\*total V5 = $175000\*78) +( A2\*total V5 = $18750\*78) +(A4\*total V5 = $8000\*78) +(A10\*total V2 = $3000\*78) +(A11\*total V2 = $30000\*78)] /100 = $214305 < $274750

Risk due to V6: [(A1\*total V6 = $40000\*79) +( A3\*total V6 = $175000\*79) +(A2\*total V6 = $18750\*79) +(A4\*total V6 = $8000\*79) +(A10\*total V2 = $3000\*79) +(A11\*total V2 = $30000\*79)] / 100 = $217052 < $274750

Risk due to V8: [(A1\*total V8 = $40000\*83) +( A3\*total V8 = $175000\*83) +(A2\*total V8 = $18750\*83) +(A4\*total V8 = $8000\*83) +(A10\*total V8 = $3000\*83) +(A11\*total V8 = $30000\*83)] / 100 = $228042 < $274750

**Ranking of Residual Asset Security Risk**:

Rank 1: A3$687750)

Rank 2: A1 ($157200)

Rank 3: A11 ($117900)

Rank 4: A2 ($73687)

Rank 5: A4 ($31440)

Rank 6: A10 ($11790)

**Ranking of Residual Vulnerability Security Risk**:

Rank 1: V8 ($228042)

Rank 2: V2 ($224495)

Rank 3: V6 ($217052)

Rank 4: V5 ($214305)

Rank 5: V4 ($195072)

**Security Risk Prevention Strategy Step P2**: Apply additional Hardening Controls (for example 2- Factor Authentication) to the highest-ranked Vulnerability Risk, with further reduced probabilities, thus further reducing the overall security asset residual risk and creating a new ranking of vulnerability security risks.

Password-based management (V8) could be a serious problem if the passwords are small or easy to catch. So, there should be some rules for a password to set up to make a strong and qualified password. 2-factor authentication is required to increase security. Modern Artificial Intelligence like fingerprint scanners, facial recognition can also add added security.

**Threat-Vulnerability pairs**:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 | **V8** |
| T1 | 14 | 17 | 14 | 16 | **14** |
| T2 | 15 | 15 | 19 | 20 | **10** |
| T4 | 16 | 14 | 15 | 15 | **11** |
| T6 | 18 | 13 | 17 | 17 | **11** |
| T5 | 19 | 12 | 13 | 11 | **9** |

**Risk Impact Matrix**:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1V2 | T1V4 | T1V5 | T1V6 | T1V8 | T2V2 | T2V4 | T2V5 | T2V6 | T2V8 | T4V2 | T4V4 | T4V5 | T4V6 | T4V8 | T6V2 | T6V4 | T6V5 | T6V6 | T6V8 | T5V2 | T5V4 | | T5V5 | | T5V6 | | T5V8 | |
| A1 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 55 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | | 100 | | 100 | |
| A3 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | | 100 | | 100 | |
| A2 | 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 | |
| A4 | 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 | |
| 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 | |
| A11 | 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 | |

**Calculating Residual Asset Security Risk**:

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Asset Value | Total Threat | Residual Asset Security Risk = (Asset\*Total Threat) /100 |
| A1 | $40000 | 365 | $146000 |
| A3 | $175000 | 365 | $638750 |
| A2 | $18750 | 365 | $68437 |
| A4 | $8000 | 365 | $29200 |
| A10 | $3000 | 365 | $10950 |
| A11 | $30000 | 365 | $109500 |

**Calculating Residual Vulnerability Security Risk**:

Risk due to V2: [(A1\*total V2 = $40000\*82) +(A3\*total V2 = $175000\*82) +(A2\*total V2 = $18750\*82) +(A4\*total V2 = $8000\*82) +(A10\*total V2 = $3000\*82) +(A11\*total V2 = $30000\*82)] / 100 = $224495 < $274750

Risk due to V4: [(A1\*total V4 = $40000\*71) +( A3\*total V4 = $175000\*71) +( A2\*total V4 = $18750\*71) +(A4\*total V4 = $8000\*71) +(A10\*total V2 = $3000\*71) +(A11\*total V2 = $30000\*71)] / 100 = $195072 < $274750

Risk due to V5: [(A1\*total V5 = $40000\*78) +( A3\*total V5 = $175000\*78) +( A2\*total V5 = $18750\*78) +(A4\*total V5 = $8000\*78) +(A10\*total V2 = $3000\*78) +(A11\*total V2 = $30000\*78)] /100 = $214305 < $274750

Risk due to V6: [(A1\*total V6 = $40000\*79) +( A3\*total V6 = $175000\*79) +(A2\*total V6 = $18750\*79) +(A4\*total V6 = $8000\*79) +(A10\*total V2 = $3000\*79) +(A11\*total V2 = $30000\*79)] / 100 = $217052 < $274750

Risk due to V8: [(A1\*total V8 = $40000\*55) +( A3\*total V8 = $175000\*55) +(A2\*total V8 = $18750\*55) +(A4\*total V8 = $8000\*55) +(A10\*total V8 = $3000\*55) +(A11\*total V8 = $30000\*55)] / 100 = $151112 < $274750

**Ranking of Residual Asset Security Risk**:

Rank 1: A3 ($638750)

Rank 2: A1 ($146000)

Rank 3: A11 ($109500)

Rank 4: A2 ($68437)

Rank 5: A4 ($29200)

Rank 6: A10 ($10950)

**Ranking of Residual Vulnerability Security Risk**:

Rank 1: V2 (($224495)

Rank 2: V6 ($217052)

Rank 3: V5 ($214305)

Rank 4: V4 ($195072)

Rank 5: V8 ($151112)

**Security Risk Prevention Strategy Step P3**: Apply additional Hardening Controls to new now highest ranked Vulnerability Risk, thus further reducing the security asset residual risks and creating a new ranking of vulnerability security risks. Using Relays in WAN server(V2) is having more residual risk from the above case. Security officials should be present to monitor data at such relay points, conducting security scans to protect data.

**Threat-Vulnerability Pairs**:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | **V2** | V4 | V5 | V6 | V8 |
| T1 | **10** | 17 | 14 | 16 | 14 |
| T2 | **9** | 15 | 19 | 20 | 10 |
| T4 | **8** | 14 | 15 | 15 | 11 |
| T6 | **7** | 13 | 17 | 17 | 11 |
| T5 | **10** | 12 | 13 | 11 | 9 |

**Risk Impact Matrix**:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1V2 | T1V4 | T1V5 | T1V6 | T1V8 | T2V2 | T2V4 | T2V5 | T2V6 | T2V8 | T4V2 | T4V4 | T4V5 | T4V6 | T4V8 | T6V2 | T6V4 | T6V5 | T6V6 | T6V8 | T5V2 | T5V4 | | T5V5 | | T5V6 | | T5V8 | |
| A1 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 55 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | | 100 | | 100 | |
| A3 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | 100 | | 100 | | 100 | |
| A2 | 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 | |
| A4 | 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 | |
| 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 | |
| A11 | 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 | |

**Calculating Residual Asset Security Risk**:

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Asset Value | Total Threat | Residual Asset Security Risk = (Asset\*Total Threat) /100 |
| A1 | $40000 | 327 | $130800 |
| A3 | $175000 | 327 | $572250 |
| A2 | $18750 | 327 | $61312 |
| A4 | $8000 | 327 | $26160 |
| A10 | $3000 | 327 | $9810 |
| A11 | $30000 | 327 | $98100 |

**Calculating Residual Vulnerability Security Risk**:

Risk due to V2: [(A1\*total V2 = $40000\*44) +(A3\*total V2 = $175000\*44) +(A2\*total V2 = $18750\*44) +(A4\*total V2 = $8000\*44) +(A10\*total V2 = $3000\*44) +(A11\*total V2 = $30000\*44)] / 100 = $120890 < $274750

Risk due to V4: [(A1\*total V4 = $40000\*71) +( A3\*total V4 = $175000\*71) +( A2\*total V4 = $18750\*71) +(A4\*total V4 = $8000\*71) +(A10\*total V2 = $3000\*71) +(A11\*total V2 = $30000\*71)] / 100 = $195072 < $274750

Risk due to V5: [(A1\*total V5 = $40000\*78) +( A3\*total V5 = $175000\*78) +( A2\*total V5 = $18750\*78) +(A4\*total V5 = $8000\*78) +(A10\*total V2 = $3000\*78) +(A11\*total V2 = $30000\*78)] /100 = $214305 < $274750

Risk due to V6: [(A1\*total V6 = $40000\*79) +( A3\*total V6 = $175000\*79) +(A2\*total V6 = $18750\*79) +(A4\*total V6 = $8000\*79) +(A10\*total V2 = $3000\*79) +(A11\*total V2 = $30000\*79)] / 100 = $217052 < $274750

Risk due to V8: [(A1\*total V8 = $40000\*55) +( A3\*total V8 = $175000\*55) +(A2\*total V8 = $18750\*55) +(A4\*total V8 = $8000\*55) +(A10\*total V8 = $3000\*55) +(A11\*total V8 = $30000\*55)] / 100 = $151112 < $274750

**Ranking of Residual Asset Security Risk**:

Rank 1: A3 ($572250)

Rank 2: A1 ($130800)

Rank 3: A11 ($98100)

Rank 4: A2 ($61312)

Rank 5: A4 ($26160)

Rank 6: A10 ($9810)

**Ranking of Residual Vulnerability Security Risk**:

Rank 1: V6 ($217052)

Rank 2: V5 ($214305)

Rank 3: V4 ($195072)

Rank 4: V8 ($151112)

Rank 5: V2 ($120890)

**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**

All the different types of controls have a common goal of decreasing the possible risk on HGA. There will be many threats that exploit vulnerabilities and damage the assets. These prevention controls assist HGA to improve their methods and work efficiently. However, risk cannot be removed completely. Hence, upgrading the policies and controls is necessary and compliance is important. Adopting too many controls can also cause confusion. Hence, controls must be selected according to the dimensions of the organization.

**Security Risk Response Strategy**

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

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

Here, we will consider the threat-vulnerability pair table from P3 with probabilities getting reduced for other vulnerabilities as well by using the M-O-T controls.

|  |  |  |
| --- | --- | --- |
| Management | Operational | Technical |
| Policies | Personnel/User Issues | Identification and Authentication |
| Life Cycle Planning | Incident Reporting and Handling | Login Access Control |
| Program Management | Awareness, Training, and Education | Cryptography |
| Risk Management | Physical and Environmental Security | Audit Trails |

**Threat-Vulnerability Pairs**:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 | V8 |
| T1 | 8 | 9 | 8 | 7 | 9 |
| T2 | 7 | 8 | 7 | 6 | 8 |
| T4 | 5 | 6 | 5 | 5 | 7 |
| T6 | 4 | 7 | 9 | 3 | 5 |
| T5 | 3 | 5 | 4 | 4 | 4 |

**Updated Risk Impact Matrix**:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1V2 | T1V4 | T1V5 | T1V6 | T1V8 | T2V2 | T2V4 | T2V5 | T2V6 | T2V8 | T4V2 | T4V4 | T4V5 | T4V6 | T4V8 | T6V2 | T6V4 | T6V5 | T6V6 | T6V8 | T5V2 | T5V4 | | T5V5 | | T5V6 | | T5V8 | |
| A1 | 65 | 50 | 40 | 55 | 50 | 60 | 45 | 35 | 50 | 45 | 40 | 60 | 50 | 55 | 50 | 35 | 30 | 25 | 50 | 30 | 35 | 50 | 45 | | 55 | | 30 | |
| A3 | 50 | 35 | 55 | 40 | 45 | 50 | 30 | 40 | 65 | 40 | 30 | 55 | 40 | 30 | 35 | 40 | 55 | 40 | 60 | 40 | 45 | 30 | 55 | | 45 | | 35 | |
| A2 | 55 | 40 | 35 | 60 | 40 | 40 | 60 | 50 | 35 | 55 | 50 | 45 | 35 | 55 | 45 | 65 | 25 | 30 | 55 | 35 | 50 | 45 | 50 | | 30 | | 40 | |
| A4 | 40 | 60 | 30 | 55 | 30 | 35 | 55 | 30 | 45 | 35 | 60 | 30 | 60 | 45 | 40 | 30 | 40 | 50 | 40 | 45 | 40 | 35 | 30 | | 40 | | 50 | |
| A10 | 45 | 35 | 30 | 35 | 40 | 45 | 40 | 55 | 50 | 30 | 35 | 40 | 45 | 50 | 55 | 45 | 35 | 30 | 45 | 40 | 35 | 30 | 35 | | 45 | | 40 | |
| A11 | 30 | 55 | 40 | 45 | 50 | 55 | 30 | 25 | 35 | 45 | 50 | 55 | 35 | 30 | 45 | 40 | 55 | 40 | 50 | 55 | 35 | 30 | 45 | | 40 | | 50 | |

**Calculation of Residual Asset Security Risk**:

For Asset A1: [$40000\*(8\*65+9\*50+8\*40+55\*7+9\*50+7\*60+8\*45+7\*35+6\*50+8\*45+5\*40+6\*60+5\*50+5\*55+7\*50+4\*35+7\*30+9\*25+3\*50+5\*30+3\*35+5\*50+4\*45+4\*55+4\*30)]/10000 = $**27980 < $40000**

For Asset A3: [$175000\*(8\*50+9\*35+8\*55+40\*7+9\*45+7\*50+8\*30+7\*40+6\*65+8\*40+5\*30+6\*55+5\*40+5\*30+7\*35+4\*40+7\*55+9\*40+3\*30+5\*40+3\*40+5\*30+4\*55+4\*45+4\*35)]/10000 = **$113750 < $175000**

For Asset A2: [$18750\*(8\*55+9\*40+8\*35+60\*7+9\*40+7\*40+8\*60+7\*50+6\*35+8\*55+5\*50+6\*45+5\*35+5\*55+7\*45+4\*65+7\*25+9\*30+3\*55+5\*35+3\*50+5\*45+4\*50+4\*30+4\*40)]/10000 = **$12759 < $18750**

For Asset A4: [$8000\*(8\*40+9\*60+8\*30+55\*7+9\*30+7\*35+8\*55+7\*30+6\*45+8\*35+5\*60+6\*30+5\*60+5\*45+7\*40+4\*30+7\*40+9\*50+3\*40+5\*45+3\*40+5\*35+4\*30+4\*40+4\*50)]/10000 = **$5164 < $8000**

For Asset A10: [$3000\*(8\*45+9\*35+8\*30+35\*7+9\*40+7\*45+8\*40+7\*55+6\*50+8\*30+5\*35+6\*40+5\*45+5\*50+7\*55+4\*45+7\*35+9\*30+3\*45+5\*40+3\*35+5\*30+4\*35+4\*45+4\*40)]/10000 = **$1836< $3000**

For Asset A11: [$30000\*(8\*30+9\*55+8\*40+45\*7+9\*50+7\*55+8\*30+7\*25+6\*35+8\*45+5\*50+6\*55+5\*35+5\*30+7\*45+4\*40+7\*55+9\*40+3\*50+5\*55+3\*35+5\*30+4\*45+4\*40+4\*50)]/10000 = **$19605< $30000**

**For all the above Assets, there is Partial Asset loss as the risk is less than the Asset value.**

**Calculation of Residual Vulnerability Security Risk**:

For V2: 40000\*(8\*65+7\*60+5\*40+4\*35+3\*35) +175000\*(8\*50+7\*50+5\*30+4\*40+3\*45) +18750\*(8\*55+7\*40+5\*50+4\*65+3\*50)+8000\*(8\*40+7\*35+5\*60+4\*30+3\*40)+3000\*(8\*45+7\*45+5\*35+4\*45+3\*35)+30000\*(8\*30+7\*55+5\*50+4\*40+3\*35)/10000 = $33684

For V4: 40000\*(8\*50+7\*45+5\*60+4\*30+3\*50) +175000\*(8\*35+7\*30+5\*55+4\*55+3\*30) +18750\*(8\*40+7\*60+5\*45+4\*25+3\*45)+8000\*(8\*60+7\*55+5\*30+4\*40+3\*35)+3000\*(8\*35+7\*40+5\*40+4\*35+3\*30)+30000\*(8\*55+7\*30+5\*55+4\*55+3\*30)/10000=$31228

For V5: 40000\*(8\*40+7\*35+5\*50+4\*25+3\*45) +175000\*(8\*55+7\*40+5\*40+4\*40+3\*55) +18750\*(8\*35+7\*50+5\*35+4\*30+3\*50)+8000\*(8\*30+7\*30+5\*60+4\*50+3\*30)+3000\*(8\*30+7\*55+5\*45+4\*30+3\*35)+30000\*(8\*40+7\*25+5\*35+4\*40+3\*45)/10000=$32052

For V6: 40000\*(8\*55+7\*50+5\*55+4\*50+3\*55) +175000\*(8\*40+7\*65+5\*30+4\*60+3\*45) +18750\*(8\*60+7\*35+5\*55+4\*55+3\*30)+8000\*(8\*55+7\*45+5\*45+4\*40+3\*40)+3000\*(8\*35+7\*50+5\*50+4\*45+3\*45)+30000\*(8\*45+7\*35+5\*30+4\*50+3\*40)/10000=$35517

For V8: 40000\*(8\*50+7\*45+5\*50+4\*30+3\*30) +175000\*(8\*45+7\*40+5\*35+4\*40+3\*35) +18750\*(8\*40+7\*55+5\*45+4\*35+3\*40)+8000\*(8\*30+7\*35+5\*40+4\*45+3\*50)+3000\*(8\*40+7\*30+5\*55+4\*40+3\*40)+30000\*(8\*50+7\*45+5\*45+4\*45+3\*50)/10000=$30778

**Ranking of Residual Asset Security Risk**:

Rank 1: A3 ($113750)

Rank 2: A1 ($27980)

Rank 3: A11 ($19605)

Rank 4: A2 ($12759)

Rank 5: A4 ($5164)

Rank 6: A10 ($1836)

**Ranking of Residual Vulnerability Security Risk**:

Rank 1: V6 ($35517)

Rank 2: V2 ($33684)

Rank 3: V5 ($32052)

Rank 4: V4 ($31228)

Rank 5: V8 ($30778)

**Security Risk Response (Resilience) Strategy Step R2**: Apply additional Hardening Controls (for example restricting services or adding a redundant server) to highest-ranked Residual Asset Risk, thus further reducing risk impact probabilities, reducing the overall security asset residual risk, and creating a new ranking of vulnerability security risks.

The highest-ranked Asset from R1 is Personnel Information(A3). By adding extra hardening controls like backing up the information in cloud or hard disks, password login, 2-factor authentication, we can protect such sensitive information.

**Taking threat-vulnerability pair**:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 | V8 |
| T1 | 8 | 9 | 8 | 7 | 9 |
| T2 | 7 | 8 | 7 | 6 | 8 |
| T4 | 5 | 6 | 5 | 5 | 7 |
| T6 | 4 | 7 | 9 | 3 | 5 |
| T5 | 3 | 5 | 4 | 4 | **4** |

Updated Matrix:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1V2 | T1V4 | T1V5 | T1V6 | T1V8 | T2V2 | T2V4 | T2V5 | T2V6 | T2V8 | T4V2 | T4V4 | T4V5 | T4V6 | T4V8 | T6V2 | T6V4 | T6V5 | T6V6 | T6V8 | T5V2 | T5V4 | | T5V5 | | T5V6 | | T5V8 | |
| A1 | 65 | 50 | 40 | 55 | 50 | 60 | 45 | 35 | 50 | 45 | 40 | 60 | 50 | 55 | 50 | 35 | 30 | 25 | 50 | 30 | 35 | 50 | 45 | | 55 | | 30 | |
| **A3** | **5** | **5** | **5** | **10** | **5** | **5** | **10** | **10** | **5** | **10** | **5** | **5** | **10** | **5** | **5** | **10** | **5** | **5** | **15** | **5** | **10** | **5** | **10** | | **5** | | **5** | |
| A2 | 55 | 40 | 35 | 60 | 40 | 40 | 60 | 50 | 35 | 55 | 50 | 45 | 35 | 55 | 45 | 65 | 25 | 30 | 55 | 35 | 50 | 45 | 50 | | 30 | | 40 | |
| A4 | 40 | 60 | 30 | 55 | 30 | 35 | 55 | 30 | 45 | 35 | 60 | 30 | 60 | 45 | 40 | 30 | 40 | 50 | 40 | 45 | 40 | 35 | 30 | | 40 | | 50 | |
| A10 | 45 | 35 | 30 | 35 | 40 | 45 | 40 | 55 | 50 | 30 | 35 | 40 | 45 | 50 | 55 | 45 | 35 | 30 | 45 | 40 | 35 | 30 | 35 | | 45 | | 40 | |
| A11 | 30 | 55 | 40 | 45 | 50 | 55 | 30 | 25 | 35 | 45 | 50 | 55 | 35 | 30 | 45 | 40 | 55 | 40 | 50 | 55 | 35 | 30 | 45 | | 40 | | 50 | |

**Calculation of Residual Asset Security Risk**:

For Asset A1: [$40000\*(8\*65+9\*50+8\*40+55\*7+9\*50+7\*60+8\*45+7\*35+6\*50+8\*45+5\*40+6\*60+5\*50+5\*55+7\*50+4\*35+7\*30+9\*25+3\*50+5\*30+3\*35+5\*50+4\*45+4\*55+4\*30)]/10000 = $**27980 < $40000**

**For Asset A3: [$175000\*(8\*5+9\*5+8\*5+10\*7+9\*5+7\*5+8\*10+7\*10+6\*5+8\*10+5\*5+6\*5+5\*10+5\*5+7\*5+4\*10+7\*5+9\*5+3\*15+5\*5+3\*10+5\*5+4\*10+4\*5+4\*5)]/10000 = $17937 < $175000**

For Asset A2: [$18750\*(8\*55+9\*40+8\*35+60\*7+9\*40+7\*40+8\*60+7\*50+6\*35+8\*55+5\*50+6\*45+5\*35+5\*55+7\*45+4\*65+7\*25+9\*30+3\*55+5\*35+3\*50+5\*45+4\*50+4\*30+4\*40)]/10000 = **$12759 < $18750**

For Asset A4: [$8000\*(8\*40+9\*60+8\*30+55\*7+9\*30+7\*35+8\*55+7\*30+6\*45+8\*35+5\*60+6\*30+5\*60+5\*45+7\*40+4\*30+7\*40+9\*50+3\*40+5\*45+3\*40+5\*35+4\*30+4\*40+4\*50)]/10000 = **$5164 < $8000**

For Asset A10: [$3000\*(8\*45+9\*35+8\*30+35\*7+9\*40+7\*45+8\*40+7\*55+6\*50+8\*30+5\*35+6\*40+5\*45+5\*50+7\*55+4\*45+7\*35+9\*30+3\*45+5\*40+3\*35+5\*30+4\*35+4\*45+4\*40)]/10000 = **$1836< $3000**

For Asset A11: [$30000\*(8\*30+9\*55+8\*40+45\*7+9\*50+7\*55+8\*30+7\*25+6\*35+8\*45+5\*50+6\*55+5\*35+5\*30+7\*45+4\*40+7\*55+9\*40+3\*50+5\*55+3\*35+5\*30+4\*45+4\*40+4\*50)]/10000 = **$19605< $30000**

**Calculation of Residual Vulnerability Security Risk**:

For V2: 40000\*(8\*65+7\*60+5\*40+4\*35+3\*35) +175000\*(8\*5+7\*5+5\*5+4\*10+3\*10) +18750\*(8\*55+7\*40+5\*50+4\*65+3\*50)+8000\*(8\*40+7\*35+5\*60+4\*30+3\*40)+3000\*(8\*45+7\*45+5\*35+4\*45+3\*35)+30000\*(8\*30+7\*55+5\*50+4\*40+3\*35)/10000 = $15747

For V4: 40000\*(8\*50+7\*45+5\*60+4\*30+3\*50) +175000\*(8\*5+7\*10+5\*5+4\*5+3\*5) +18750\*(8\*40+7\*60+5\*45+4\*25+3\*45)+8000\*(8\*60+7\*55+5\*30+4\*40+3\*35)+3000\*(8\*35+7\*40+5\*40+4\*35+3\*30)+30000\*(8\*55+7\*30+5\*55+4\*55+3\*30)/10000=$15391

For V5: 40000\*(8\*40+7\*35+5\*50+4\*25+3\*45) +175000\*(8\*5+7\*10+5\*10+4\*5+3\*10) +18750\*(8\*35+7\*50+5\*35+4\*30+3\*50)+8000\*(8\*30+7\*30+5\*60+4\*50+3\*30)+3000\*(8\*30+7\*55+5\*45+4\*30+3\*35)+30000\*(8\*40+7\*25+5\*35+4\*40+3\*45)/10000=$13940

For V6: 40000\*(8\*55+7\*50+5\*55+4\*50+3\*55) +175000\*(8\*10+7\*5+5\*5+4\*15+3\*5) +18750\*(8\*60+7\*35+5\*55+4\*55+3\*30)+8000\*(8\*55+7\*45+5\*45+4\*40+3\*40)+3000\*(8\*35+7\*50+5\*50+4\*45+3\*45)+30000\*(8\*45+7\*35+5\*30+4\*50+3\*40)/10000=$16530

For V8: 40000\*(8\*50+7\*45+5\*50+4\*30+3\*30) +175000\*(8\*5+7\*10+5\*5+4\*5+3\*5) +18750\*(8\*40+7\*55+5\*45+4\*35+3\*40)+8000\*(8\*30+7\*35+5\*40+4\*45+3\*50)+3000\*(8\*40+7\*30+5\*55+4\*40+3\*40)+30000\*(8\*50+7\*45+5\*45+4\*45+3\*50)/10000=$14853

**Ranking of Residual Asset Security Risk**:

Rank 1: A1 ($27980)

Rank 2: A11 ($19605)

Rank 3: A3 ($17937)

Rank 4: A2 ($12759)

Rank 5: A4 ($5164)

Rank 6: A10 ($1836)

**Ranking of Residual Vulnerability Security Risk**:

Rank 1: V6 ($16530)

Rank 2: V2 ($15747)

Rank 3: V4 ($15391)

Rank 4: V8 ($14853)

Rank 5: V5 ($13940)

**Security Risk Response (Resilience) Strategy Step R3**: Apply additional Hardening Controls to new now highest ranked Residual Asset Risk, thus reducing risk impact probabilities, further reducing the overall security asset residual risk, and creating a new ranking of vulnerability security risks.

Now considering the highest rank asset from the above case which is a LAN Server(A1) and applying hardening controls like maintaining virus protection software, doing scans from time to time, password protection, information backup will help to protect the asset.

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 | V8 |
| T1 | 8 | 9 | 8 | 7 | 9 |
| T2 | 7 | 8 | 7 | 6 | 8 |
| T4 | 5 | 6 | 5 | 5 | 7 |
| T6 | 4 | 7 | 9 | 3 | 5 |
| T5 | 3 | 5 | 4 | 4 | **4** |

**Risk Matrix**:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1V2 | T1V4 | T1V5 | T1V6 | T1V8 | T2V2 | T2V4 | T2V5 | T2V6 | T2V8 | T4V2 | T4V4 | T4V5 | T4V6 | T4V8 | T6V2 | T6V4 | T6V5 | T6V6 | T6V8 | T5V2 | T5V4 | | T5V5 | | T5V6 | | T5V8 | |
| **A1** | **10** | **5** | **15** | **10** | **5** | **15** | **10** | **5** | **15** | **10** | **5** | **15** | **10** | **5** | **15** | **10** | **5** | **15** | **10** | **5** | **15** | **10** | **5** | | **15** | | **5** | |
| A3 | 5 | 5 | 5 | 10 | 5 | 5 | 10 | 10 | 5 | 10 | 5 | 5 | 10 | 5 | 5 | 10 | 5 | 5 | 15 | 5 | 10 | 5 | 10 | | 5 | | 5 | |
| A2 | 55 | 40 | 35 | 60 | 40 | 40 | 60 | 50 | 35 | 55 | 50 | 45 | 35 | 55 | 45 | 65 | 25 | 30 | 55 | 35 | 50 | 45 | 50 | | 30 | | 40 | |
| A4 | 40 | 60 | 30 | 55 | 30 | 35 | 55 | 30 | 45 | 35 | 60 | 30 | 60 | 45 | 40 | 30 | 40 | 50 | 40 | 45 | 40 | 35 | 30 | | 40 | | 50 | |
| A10 | 45 | 35 | 30 | 35 | 40 | 45 | 40 | 55 | 50 | 30 | 35 | 40 | 45 | 50 | 55 | 45 | 35 | 30 | 45 | 40 | 35 | 30 | 35 | | 45 | | 40 | |
| A11 | 30 | 55 | 40 | 45 | 50 | 55 | 30 | 25 | 35 | 45 | 50 | 55 | 35 | 30 | 45 | 40 | 55 | 40 | 50 | 55 | 35 | 30 | 45 | | 40 | | 50 | |

**Calculation of Residual Asset Security Risk**:

**For Asset A1: [$40000\*(8\*10+9\*5+8\*15+10\*7+9\*5+7\*15+8\*10+7\*5+6\*15+8\*10+5\*5+6\*15+5\*10+5\*5+7\*15+4\*10+7\*5+9\*15+3\*10+5\*5+3\*15+5\*10+4\*5+4\*15+4\*5)]/10000 = $6020 < $40000**

For Asset A3: [$175000\*(8\*5+9\*5+8\*5+10\*7+9\*5+7\*5+8\*10+7\*10+6\*5+8\*10+5\*5+6\*5+5\*10+5\*5+7\*5+4\*10+7\*5+9\*5+3\*15+5\*5+3\*10+5\*5+4\*10+4\*5+4\*5)]/10000 = **$17937 < $175000**

For Asset A2: [$18750\*(8\*55+9\*40+8\*35+60\*7+9\*40+7\*40+8\*60+7\*50+6\*35+8\*55+5\*50+6\*45+5\*35+5\*55+7\*45+4\*65+7\*25+9\*30+3\*55+5\*35+3\*50+5\*45+4\*50+4\*30+4\*40)]/10000 = **$12759 < $18750**

For Asset A4: [$8000\*(8\*40+9\*60+8\*30+55\*7+9\*30+7\*35+8\*55+7\*30+6\*45+8\*35+5\*60+6\*30+5\*60+5\*45+7\*40+4\*30+7\*40+9\*50+3\*40+5\*45+3\*40+5\*35+4\*30+4\*40+4\*50)]/10000 = **$5164 < $8000**

For Asset A10: [$3000\*(8\*45+9\*35+8\*30+35\*7+9\*40+7\*45+8\*40+7\*55+6\*50+8\*30+5\*35+6\*40+5\*45+5\*50+7\*55+4\*45+7\*35+9\*30+3\*45+5\*40+3\*35+5\*30+4\*35+4\*45+4\*40)]/10000 = **$1836< $3000**

For Asset A11: [$30000\*(8\*30+9\*55+8\*40+45\*7+9\*50+7\*55+8\*30+7\*25+6\*35+8\*45+5\*50+6\*55+5\*35+5\*30+7\*45+4\*40+7\*55+9\*40+3\*50+5\*55+3\*35+5\*30+4\*45+4\*40+4\*50)]/10000 = **$19605< $30000**

**Calculation of Residual Vulnerability Security Risk**:

For V2: 40000\*(8\*10+7\*15+5\*5+4\*10+3\*15) +175000\*(8\*5+7\*5+5\*5+4\*10+3\*10) +18750\*(8\*55+7\*40+5\*50+4\*65+3\*50)+8000\*(8\*40+7\*35+5\*60+4\*30+3\*40)+3000\*(8\*45+7\*45+5\*35+4\*45+3\*35)+30000\*(8\*30+7\*55+5\*50+4\*40+3\*35)/10000 = $11387

For V4: 40000\*(8\*5+7\*10+5\*15+4\*5+3\*10) +175000\*(8\*5+7\*10+5\*5+4\*5+3\*5) +18750\*(8\*40+7\*60+5\*45+4\*25+3\*45)+8000\*(8\*60+7\*55+5\*30+4\*40+3\*35)+3000\*(8\*35+7\*40+5\*40+4\*35+3\*30)+30000\*(8\*55+7\*30+5\*55+4\*55+3\*30)/10000=$11191

For V5: 40000\*(8\*15+7\*5+5\*10+4\*15+3\*5) +175000\*(8\*5+7\*10+5\*10+4\*5+3\*10) +18750\*(8\*35+7\*50+5\*35+4\*30+3\*50)+8000\*(8\*30+7\*30+5\*60+4\*50+3\*30)+3000\*(8\*30+7\*55+5\*45+4\*30+3\*35)+30000\*(8\*40+7\*25+5\*35+4\*40+3\*45)/10000=$10860

For V6: 40000\*(8\*10+7\*15+5\*5+4\*10+3\*15) +175000\*(8\*10+7\*5+5\*5+4\*15+3\*5) +18750\*(8\*60+7\*35+5\*55+4\*55+3\*30)+8000\*(8\*55+7\*45+5\*45+4\*40+3\*40)+3000\*(8\*35+7\*50+5\*50+4\*45+3\*45)+30000\*(8\*45+7\*35+5\*30+4\*50+3\*40)/10000=$11990

For V8: 40000\*(8\*5+7\*10+5\*15+4\*5+3\*5) +175000\*(8\*5+7\*10+5\*5+4\*5+3\*5) +18750\*(8\*40+7\*55+5\*45+4\*35+3\*40)+8000\*(8\*30+7\*35+5\*40+4\*45+3\*50)+3000\*(8\*40+7\*30+5\*55+4\*40+3\*40)+30000\*(8\*50+7\*45+5\*45+4\*45+3\*50)/10000=$11033

**Ranking of Residual Asset Security Risk**:

Rank 1: A11 ($19605)

Rank 2: A3 ($17937)

Rank 3: A2 ($12759)

Rank 4: A1 ($6020)

Rank 5: A4 ($5164)

Rank 6: A10 ($1836)

**Ranking of Residual Vulnerability Security Risk**:

Rank 1: V6 ($11990)

Rank 2: V2 ($11387)

Rank 3: V4 ($11191)

Rank 4: V8 ($11033)

Rank 5: V5 ($10860)

**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**

All the different types of controls have a common goal of decreasing the possible risk on HGA. There will be many threats that exploit vulnerabilities and damage the assets. These prevention controls assist HGA to improve their methods and work efficiently. However, risk cannot be removed completely. Hence, upgrading the policies and controls is necessary and compliance is important. Adopting too many controls can also cause confusion. Hence, controls must be selected according to the dimensions of the organization.

**Mixed Strategy**:

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

By following the mixed strategy, the values of both threat-vulnerability probabilities and the values in the risk matrix decrease to a large extent.

**Threat-Vulnerability pair**:

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | V2 | V4 | V5 | V6 | V8 |
| T1 | 8 | 9 | 8 | 7 | 9 |
| T2 | 7 | 8 | 7 | 6 | 8 |
| T4 | 5 | 6 | 5 | 5 | 7 |
| T6 | 4 | 7 | 9 | 3 | 5 |
| T5 | 3 | 5 | 4 | 4 | **4** |

**Updated Risk Matrix**:

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
|  | T1V2 | T1V4 | T1V5 | T1V6 | T1V8 | T2V2 | T2V4 | T2V5 | T2V6 | T2V8 | T4V2 | T4V4 | T4V5 | T4V6 | T4V8 | T6V2 | T6V4 | T6V5 | T6V6 | T6V8 | T5V2 | T5V4 | | T5V5 | | T5V6 | | T5V8 | |
| A1 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | | 15 | | 5 | |
| A3 | 5 | 5 | 5 | 10 | 5 | 5 | 10 | 10 | 5 | 10 | 5 | 5 | 10 | 5 | 5 | 10 | 5 | 5 | 15 | 5 | 10 | 5 | 10 | | 5 | | 5 | |
| A2 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | | 15 | | 5 | |
| A4 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | | 15 | | 5 | |
| A10 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | | 15 | | 5 | |
| A11 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | 15 | 10 | 5 | | 15 | | 5 | |

**Calculation of Residual Asset Security Risk**:

For Asset A1: [$40000\*(8\*10+9\*5+8\*15+10\*7+9\*5+7\*15+8\*10+7\*5+6\*15+8\*10+5\*5+6\*15+5\*10+5\*5+7\*15+4\*10+7\*5+9\*15+3\*10+5\*5+3\*15+5\*10+4\*5+4\*15+4\*5)]/10000 = **$6020 < $40000**

For Asset A3: [$175000\*(8\*5+9\*5+8\*5+10\*7+9\*5+7\*5+8\*10+7\*10+6\*5+8\*10+5\*5+6\*5+5\*10+5\*5+7\*5+4\*10+7\*5+9\*5+3\*15+5\*5+3\*10+5\*5+4\*10+4\*5+4\*5)]/10000 = **$17937 < $175000**

For Asset A2: [$18750\*(8\*10+9\*5+8\*15+10\*7+9\*5+7\*15+8\*10+7\*5+6\*15+8\*10+5\*5+6\*15+5\*10+5\*5+7\*15+4\*10+7\*5+9\*15+3\*10+5\*5+3\*15+5\*10+4\*5+4\*15+4\*5)]/10000 = **$2821 < $18750**

For Asset A4: [$8000\*(8\*10+9\*5+8\*15+10\*7+9\*5+7\*15+8\*10+7\*5+6\*15+8\*10+5\*5+6\*15+5\*10+5\*5+7\*15+4\*10+7\*5+9\*15+3\*10+5\*5+3\*15+5\*10+4\*5+4\*15+4\*5)]/10000 = **$1204 < $8000**

For Asset A10: [$3000\*(8\*10+9\*5+8\*15+10\*7+9\*5+7\*15+8\*10+7\*5+6\*15+8\*10+5\*5+6\*15+5\*10+5\*5+7\*15+4\*10+7\*5+9\*15+3\*10+5\*5+3\*15+5\*10+4\*5+4\*15+4\*5)]/10000 = **$451< $3000**

For Asset A11: [$30000\*(8\*10+9\*15+8\*15+10\*7+9\*5+7\*15+8\*10+7\*5+6\*15+8\*10+5\*5+6\*15+5\*10+5\*5+7\*15+4\*10+7\*5+9\*15+3\*10+5\*5+3\*15+5\*10+4\*5+4\*15+4\*5)]/10000 = **$4515< $30000**

**Calculation of Residual Vulnerability Security Risk**:

For V2: 40000\*(8\*10+7\*15+5\*5+4\*10+3\*15) +175000\*(8\*5+7\*5+5\*5+4\*10+3\*10) +18750\*(8\*10+7\*15+5\*5+4\*10+3\*15)+8000\*(8\*10+7\*15+5\*5+4\*10+3\*15)+3000\*(8\*10+7\*15+5\*5+4\*10+3\*15)+30000\*(8\*10+7\*15+5\*5+4\*10+3\*15)/10000 = $5917

For V4: 40000\*(8\*5+7\*10+5\*15+4\*5+3\*10) +175000\*(8\*5+7\*10+5\*5+4\*5+3\*5) +18750\*(8\*5+7\*10+5\*15+4\*5+3\*10)+8000\*(8\*5+7\*10+5\*15+4\*5+3\*10)+3000\*(8\*5+7\*10+5\*15+4\*5+3\*10)+30000\*(8\*5+7\*10+5\*15+4\*5+3\*10)/10000=$5319

For V5: 40000\*(8\*15+7\*5+5\*10+4\*15+3\*5) +175000\*(8\*5+7\*10+5\*10+4\*5+3\*10) +18750\*(8\*15+7\*5+5\*10+4\*15+3\*5)+8000\*(8\*15+7\*5+5\*10+4\*15+3\*5)+3000\*(8\*15+7\*5+5\*10+4\*15+3\*5)+30000\*(8\*15+7\*5+5\*10+4\*15+3\*5)/10000=$6468

For V6: 40000\*(8\*10+7\*15+5\*5+4\*10+3\*15) +175000\*(8\*10+7\*5+5\*5+4\*15+3\*5) +18750\*(8\*10+7\*15+5\*5+4\*10+3\*15)+8000\*(8\*10+7\*15+5\*5+4\*10+3\*15)+3000\*(8\*10+7\*15+5\*5+4\*10+3\*15)+30000\*(8\*10+7\*15+5\*5+4\*10+3\*15)/10000=$6705

For V8: 40000\*(8\*5+7\*10+5\*15+4\*5+3\*5) +175000\*(8\*5+7\*10+5\*5+4\*5+3\*5) +18750\*(8\*5+7\*10+5\*15+4\*5+3\*5)+8000\*(8\*5+7\*10+5\*15+4\*5+3\*5)+3000\*(8\*5+7\*10+5\*15+4\*5+3\*5)+30000\*(8\*5+7\*10+5\*15+4\*5+3\*5)/10000=$5169

**Ranking of Residual Asset Security Risk**:

Rank 1: A3 ($17937)

Rank 2: A1 ($6020)

Rank 3: A11 ($4515)

Rank 4: A2 ($2821)

Rank 5: A4 ($1204)

Rank 6: A10 ($451)

**Ranking of Residual Vulnerability Security Risk**:

Rank 1: V6 ($6705)

Rank 2: V5 ($6468)

Rank 3: V2 ($5917)

Rank 4: V4 ($5319)

Rank 5: V8 ($5169)

**Conclusion: Cost-Benefit Analysis**

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

We considered a Hypothetical Government Agency based case study and categorized a list of Assets, threats, and vulnerabilities. From the main set, we have considered a subset of four from each of assets, threats, and vulnerabilities to study their impact on them. For the first scenario, we calculated residual asset security risk and residual vulnerability security risk by using the values from the threat-vulnerability table of probabilities. For the second scenario, we decreased the probabilities to some extent in the threat-vulnerability table and once again calculated residual asset and vulnerability security risk. In scenario 3, we used prevention strategies to decrease the extent of the exploitation of vulnerabilities. All these above cases included 0% system resilience. Now, resilience is increased, and a new matrix of risk probabilities is framed for response strategies. The response strategies focus on the riskier asset, and the hardening controls are applied to reduce the risk on the assets. Later we conducted a mixed strategy of both prevention and response controls. We observed the trend of how the risk on assets and vulnerabilities is reduced by applying various controls. This case study clearly explains all the information of a cyber-attack, what it includes, and what can an organization do in time of an attack. All this is understood with proof of mathematical calculations.

HGA is addressing the most important controls to decrease the threats on its assets. Much more care must be taken whether everything is complying or not. HGA must be more cautious in identifying the threats and it should constantly upgrade its policies and technology.

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

Both Prevention and Response strategies are important to face and deal with risk in any organization. Prevention strategies mainly concentrate on dealing with threats and vulnerabilities. From the above-mentioned values, various prevention controls helped to decrease the probabilities of threat and vulnerability. On the other hand, the response controls mainly focused on assets. Their focus is to protect assets after an attack is done. As observed above, the response strategies brought down the risk on the assets to a large extent. I would prefer to include more prevention strategies as they would stop any threats to exploit the vulnerabilities to some extent. But, though how many prevention strategies are employed, there will **always be a risk** in any system. Hence, response strategies also play a crucial role. Therefore, **a mixed strategy would be ideal** for a healthy operation of a company. Based upon the size and dealings of a company, it should decide the ratio of prevention to response strategies in a mixed-mode.

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

|  |  |  |  |
| --- | --- | --- | --- |
| **Controls Mitigating** | **Risk Prevention Budget** | **Risk Response Budget** | **Mixed Strategy Budget** |
| Financial Fraud | $40000 | $30000 | $45000 |
| Errors in data entry | $30000 | $25000 | $35000 |
| Malicious Employee | $20000 | $10000 | $25000 |
| Network-based problems | $40000 | $35000 | $40000 |
| Exposing crucial information | $30000 | $25000 | $35000 |
| Virtual Private Network | $25000 | $15000 | $30000 |
| Demilitarized Zone | $20000 | $20000 | $20000 |
| Total | $205000 | $160000 | $230000 |

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

**= $274750 - $32948 = $241802**

**Here, the value of risk reduction exceeds the budget for new proposed controls**

**Proposed Security Risk Budget Cost for 3 budgets:**

Cost-Benefit Ratio Analysis for Risk Prevention Budget =

Proposed Security Risk Budget Cost / Expected Security risk benefit =

$205000 / $241802 = 0.85

Cost-Benefit Ratio Analysis for Risk Response Budget =

Proposed Security Risk Budget Cost / Expected Security risk benefit =

$160000 / $241802 = 0.66

Cost-Benefit Ratio Analysis for Mixed Strategy Budget =

Proposed Security Risk Budget Cost / Expected Security risk benefit =

$230000 / $241802 = 0.95

**PART B: SECURITY RISK MANAGEMENT IMPLEMENTATION PLAN**

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

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

**List of Critical Assets:**

|  |  |  |
| --- | --- | --- |
| Asset No. | Asset Name | Asset Value |
| A1 | Personal Information | $25000 |
| A2 | Business Documents | $40000 |
| A3 | Hardware Components and Infrastructure | $30000 |
| A4 | Computers and network elements | $35000 |
| A5 | Storage elements, cloud services | $20000 |

**List of Missing Cybersecurity Controls:**

|  |
| --- |
| **Missing Controls** |
| **Personal Authentication** |
| Digital Certificates using Cryptography |
| Government ID unique numbers |
| **Authorization** |
| Control Lists |
| **Logical Access Controls Methods** |
| PKI Compliance Requirements |
| The DOD Common Access Card |
| Logical Network Port Security |
| **Physical Access Control Methods** |
| Physical Intrusion Detection Systems |
| Physical Tokens |
| **Biometric Systems** |
| Eye Scanners |

**List of Potential Vulnerabilities**

1. Easy Access
2. Information Theft
3. Unauthorized Access
4. Access to Confidential Information
5. Improper Storage and Backup

**List of Potential Threats**

1. Hacking of Potential Systems
2. Exposing Crucial Information
3. Halt in Operations
4. Irrecoverable damage to assets
5. Loss of data

**List of Possible Risks**

1. False Authentication can be possible
2. Modification of data and injection of virus into systems.
3. The weak access points in the network will be known and can be used later to enter into the systems
4. Authentication of a fake individual can be possible
5. No guarantee that the sender is actually sending the information
6. False authorization to assets within the available staff is also harmful.
7. **Network Infrastructure Security Risk Management Implementation Controls and Policies**

* Enclave Protection
* Firewalls
* Routers

**List of Critical Assets**:

|  |  |  |
| --- | --- | --- |
| Asset No. | Asset Name | Asset Value |
| A1 | Personal Information | $25000 |
| A2 | Business Documents | $40000 |
| A3 | Hardware Components and Infrastructure | $30000 |
| A4 | Computers and network elements | $35000 |
| A5 | Storage elements, cloud services | $20000 |

**List of Missing Cybersecurity Controls:**

|  |
| --- |
| **Missing Controls** |
| **Enclave Protection** |
| Use of Intrusion Detection System |
| Use of Network Test Access Ports |
| **Firewalls** |
| Screened Host |
| Hybrid Technology Firewall |
| **Routers** |
| Securing Routing Planes |

**List of Potential Vulnerabilities**

1. Easy Access
2. Information Theft
3. Unauthorized Access
4. Access to Confidential Information
5. Firewall Setting

**List of Potential Threats**

1. Hacking of Potential Systems
2. Exposing Crucial Information
3. Halt in Operations
4. Irrecoverable damage to assets
5. Loss of data

**List of Possible Risks**

1. Getting external access into systems
2. Improper organization of data packets
3. Improper routing of data packets
4. Access of unwanted cookies into the system
5. Possible DOS attack
6. **Network Infrastructure Security Risk Management Implementation Controls and Policies**

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

**List of Critical Assets**:

|  |  |  |
| --- | --- | --- |
| Asset No. | Asset Name | Asset Value |
| A1 | Personal Information | $25000 |
| A2 | Business Documents | $40000 |
| A3 | Hardware Components and Infrastructure | $30000 |
| A4 | Computers and network elements | $35000 |
| A5 | Storage elements, cloud services | $20000 |

**List of Missing Cybersecurity Controls:**

|  |
| --- |
| **Missing Controls** |
| **Ports, Protocols, and Services** |
| Unicast Reverse Path Forwarding |
| IPV6 Address Filtering |
| **Device Management** |
| Out-Of-Band Management |
| **Device Monitoring** |
| Network Management Station |
| **Network Intrusion Detection Systems (NIDS)** |
| External Network Intrusion Detection |
| **Switches and VLANs** |
| VLAN Port Security |
| VLAN 802.1x and Management Policy Server |
| **Virtual Private Network** |
| Gateway-to-Gateway |
| Host-to-Host |

**List of Potential Vulnerabilities**

1. Easy Access
2. Information Theft
3. Unauthorized Access
4. Access to Confidential Information
5. Firewall Setting

**List of Potential Threats**

1. Hacking of Potential Systems
2. Exposing Crucial Information
3. Halt in Operations
4. Irrecoverable damage to assets
5. Loss of data

**List of Possible Risks**

1. Getting external access into systems
2. Violation of unused ports and protocols
3. Trust in business with clients will be lost
4. Access of unwanted cookies into the system
5. Possible DOS attack
6. Lack of timed out option will expose the resources
7. Allowing access through improper address filtering
8. **Database Security Risk Management Implementation Controls and Policies**

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

**List of Critical Assets**:

|  |  |  |
| --- | --- | --- |
| Asset No. | Asset Name | Asset Value |
| A1 | Personal Information | $25000 |
| A2 | Business Documents | $40000 |
| A3 | Hardware Components and Infrastructure | $30000 |
| A4 | Computers and network elements | $35000 |
| A5 | Storage elements, cloud services | $20000 |

**List of Missing Cybersecurity Controls:**

|  |
| --- |
| **Missing Controls** |
| **Authentication** |
| Application User manager |
| Application Account |
| Database Auditor |
| **Authorization** |
| Renaming default accounts |
| **Confidentiality** |
| Source code encryption |
| **Auditing** |
| Audit Log Retention |
| **Replication and Federation** |
| Federated database |
| **Database Clustering** |
| Trial of accountability |
| **Operating System Protections** |
| Dedicated directories and files |
| **Application Protections** |
| Avoiding the display of unauthorized information |
| **Database Security Design and Configuration** |
| Partitioning the Application |
| Configuration Management Process |
| IA Documentation |
| Software Baseline |
| **Enclave and Computing Environment** |
| Least Privilege |
| Marking and Labeling |
| Production Code Change Controls |
| Warning Message |
| **Business Continuity** |
| Backup Copies of Critical Software |
| Trusted Recovery |

**List of Potential Vulnerabilities**

1. Easy Access
2. Information Theft
3. Unauthorized Access
4. Access to Confidential Information
5. Adding malware patch to the software
6. Exposing key information
7. Easy chance of exploitation
8. Easy availability of an access point

**List of Potential Threats**

1. Hacking of Potential Systems
2. Exposing Crucial Information
3. Halt in Operations
4. Irrecoverable damage to assets
5. Loss of data

**List of Possible Risks**

1. Getting external access into systems
2. Access of unwanted cookies into the system
3. Halt in business activities
4. Detection of theft becomes difficult
5. Suspicious insider attack can take place
6. Identification of flaws within the security plan cannot take place
7. Trust in business with clients will be lost
8. Lack of clarity in organization and working
9. **Applications Security Risk Management Implementation Controls and Policies**

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

**List of Critical Assets**:

|  |  |  |
| --- | --- | --- |
| Asset No. | Asset Name | Asset Value |
| A1 | Personal Information | $25000 |
| A2 | Business Documents | $40000 |
| A3 | Hardware Components and Infrastructure | $30000 |
| A4 | Computers and network elements | $35000 |
| A5 | Storage elements, cloud services | $20000 |

**List of Missing Cybersecurity Controls:**

|  |
| --- |
| **Missing Controls** |
| **Application Data Handling** |
| Data Marking |
| **Authentication** |
| Standalone Application Authentication |
| Server Application Authentication |
| Password Complexity and Maintenance |
| **Cryptography** |
| Use of Message Authentication Codes |
| **User Accounts** |
| Manual Unlock Policy |
| Application Sessions |
| **Input Validation** |
| Command Injection Vulnerabilities |
| Race Conditions |
| **Configuration Management** |
| Software Configuration Management |
| **Testing** |
| Web Applications Vulnerability Scanners |
| **Deployment** |
| Auditing |

**List of Potential Vulnerabilities**

1. Easy Access
2. Information Theft
3. Unauthorized Access
4. Access to Confidential Information
5. System crashing
6. Easy chance of exploitation
7. Easy availability of an access point
8. Insider Access

**List of Potential Threats**

1. Hacking of Potential Systems
2. Exposing Crucial Information
3. Halt in Operations
4. Irrecoverable damage to assets
5. Loss of data

**List of Possible Risks**

* 1. Getting external access to systems
  2. Access to unwanted cookies in the system
  3. Detection of theft becomes difficult
  4. Suspicious insider attack can take place
  5. Identification of flaws within the security plan cannot take place
  6. Lack of clarity in organization and working
  7. Password cracking becomes easy by brute force
  8. A system crash can take place

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

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

**List of Critical Assets**:

|  |  |  |
| --- | --- | --- |
| Asset No. | Asset Name | Asset Value |
| A1 | Personal Information | $25000 |
| A2 | Business Documents | $40000 |
| A3 | Hardware Components and Infrastructure | $30000 |
| A4 | Computers and network elements | $35000 |
| A5 | Storage elements, cloud services | $20000 |

**List of Missing Cybersecurity Controls:**

|  |
| --- |
| **Missing Controls** |
| **Wireless LAN Risk Management** |
| Protected Extensible Authentication Protocol |
| **Wireless PAN Risk Management** |
| Wireless PAN Standards |
| Threats |
| **Wireless WAN Risk Management** |
| Mobitex |
| **Wireless RFID Risk Management** |
| Storage of encrypted data only |
| **Wireless PED Risk Management** |
| PDA Security |

**List of Potential Vulnerabilities**

1. Easy Access
2. Information Theft
3. Unauthorized Access
4. Access to Confidential Information
5. Easy chance of exploitation
6. Easy availability of an access point
7. Insider Access

**List of Potential Threats**

1. Hacking of Potential Systems
2. Exposing Crucial Information
3. Halt in Operations
4. Irrecoverable damage to assets
5. Loss of data

**List of Possible Risks**

* 1. Getting external access to systems
  2. Access to unwanted cookies in the system
  3. Detection of theft becomes difficult
  4. Suspicious insider attack can take place
  5. Identification of flaws within the security plan cannot take place
  6. Loss in Confidentiality and Integrity

**List of Cybersecurity Implementation Controls at Kshemin Innovations PVT LTD**

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

|  |
| --- |
| Cybersecurity Implementation Controls |
| **Identification Credentials** |
| ID Card Scanning |
| Biometric Login |
| Password-based Login |
| **Personal Authentication** |
| ID Card Scanning |
| Biometric Login |
| Password-based Login |
| **Authorization** |
| Security Policies |
| Use of Security Tokens |
| **Logical Access Controls Methods** |
| Network Architecture Controls |
| Remote Network Access |
| Encryption |
| PKI Compliance Requirements |
| Passwords, PINs, and Implementations |
| Alternate Login Token |
| **Physical Access Control Methods** |
| Classified Storage and Handling |
| Access Points |
| Smart Cards |
| PINs |
| **Biometric Systems** |
| Fingerprint Scanners |

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

|  |
| --- |
| Cybersecurity Implementation Controls |
| **Enclave Protection** |
| Defense-in-depth |
| Use of Firewalls |
| Use of Routers |
| Use of DMZ |
| Use of VPN |
| **Firewalls** |
| Packet Filtering |
| Stateful Inspection Firewall |
| Application Proxy Gateway |
| **Routers** |
| Route Table Integrity |

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

|  |
| --- |
| Cybersecurity Implementation Controls |
| **Ports, Protocols, and Services** |
| Different levels of blocking protocols at the enclave perimeter |
| IPV4 Address Filtering |
| Protecting Servers or LANS against SYN Flood Attack |
| Blocking ICMPv4 echo request - echo reply and Traceroute utility |
| **Device Management** |
| Vulnerability Management System |
| In-Band-Management |
| **Device Monitoring** |
| Simple Network Management Protocol (SNMP) |
| **Network Authentication, Authorization and Accounting** |
| Authentication |
| Authorization |
| Accounting |
| Auditing |
| Routing Password Protection |
| **Network Intrusion Detection Systems (NIDS)** |
| Local Area Network Intrusion Detection |
| **Switches and VLANs** |
| Physical Switches and Wiring |
| Virtual Local Area Networks (VLANs) |
| VLAN Trunking |
| **Virtual Private Network** |
| Host-to-Gateway |

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

|  |
| --- |
| Cybersecurity Implementation Controls |
| **Authentication** |
| Database User Accounts |
| Database Administrator |
| Application Owner |
| Database Operator |
| Passwords |
| Certificates |
| External Authentication |
| Credential Storage |
| **Authorization** |
| Access based on role |
| **Confidentiality** |
| Data file encryption |
| Data encryption |
| **Data Integrity** |
| Transaction Logging |
| Transaction Journaling |
| **Auditing** |
| Audit Log Protection |
| Audit Reporting |
| **Replication and Federation** |
| Database Replication |
| **Database Clustering** |
| Database Clustering |
| Protection of Communication Path |
| **Backup and Recovery** |
| Database backup and recovery testing |
| Backup data encryption |
| Access control for backup data |
| **Operating System Protections** |
| Dedicated OS accounts |
| Updated software |
| **Application Protections** |
| Audit access to sensitive data |
| Input validation |
| Requirement for Authentication |
| **Network Protections** |
| Giving access to users having requirement |
| Restricting access to users |
| Limits on network session parameters |
| **Database Security design and Configuration** |
| Procedural Review |
| Configuration Specification |
| Compliance Testing |
| Functional Architecture |
| Non-repudiation |
| System Library Management Controls |
| Security Support Structure Partitioning |
| System State Changes |
| Individual Identification and Authentication |
| Token and Certificate Standards |
| **Enclave and Computing Environment** |
| Access for Need–to–know |
| Audit Record Content |
| Audit Trail, Monitoring, Analysis, and Reporting |
| Changes to Data |
| Encryption for data at rest |
| Encryption for data in transit |
| Data Change Controls |
| Logon |
| Audit of Security Label Changes |
| Resource Control |
| Audit Record Retention |
| Security Configuration Compliance |
| Boundary Defense |
| Remote Access for Privileged Functions |
| **Business Continuity** |
| Protection of Backup and Restoration Assets |
| Data Backup Procedures |
| Disaster and Recovery Planning |
| **Vulnerability Management** |
| Vulnerability Management |

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

|  |
| --- |
| Cybersecurity Implementation Controls |
| **Application Data Handling** |
| Database management system |
| Data storage |
| In-Memory data handling |
| Data Transmission |
| Data Integrity |
| **Authentication** |
| Server Authentication |
| User Authentication |
| Signed Code Identification |
| Client Application Authentication |
| Combination Client Server Application Authentication |
| Application Component Authentication |
| PKI Certificate Validation |
| Authentication Credentials Protection |
| **Cryptography** |
| Use of Symmetric Cyphers |
| Use of Digital Signature |
| **User Accounts** |
| Mechanism to detect duplicate user accounts |
| Account Locking |
| Access Control |
| **Input Validation** |
| Integer Overflow |
| Format String Vulnerabilities |
| Buffer Overflows |
| **Application Auditing** |
| Auditing all access to need-to-know information |
| Protection of contents of audit trails |
| **Configuration Management** |
| Release Manager |
| **Testing** |
| Test Plans and Procedures |
| Automated Tools |
| **Deployment** |
| Documentation |
| Maintenance and Availability |

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

|  |
| --- |
| Cybersecurity Implementation Controls |
| **Wireless LAN Risk Management** |
| IEEE 802.1x Extensible Authentication Protocol (EAP) |
| EAP-TLS |
| EAP-TTLS |
| Lightweight Extensible Authentication Protocol |
| Wireless station |
| Wireless Network Interface Cards |
| Access Point |
| Use of VPN |
| Service Set Identifier (SSID) |
| MAC address |
| **Wireless PAN Risk Management** |
| Bluetooth Specification |
| Pairing |
| Bluetooth Security Modes |
| Secure Simple Pairing |
| **Wireless WAN Risk Management** |
| Cellular Digital Packet Data |
| Broadband Wireless Access |
| Mobile WiMAX |
| **Wireless RFID Risk Management** |
| Passive Systems |
| Active Systems |
| **Wireless PED Risk Management** |
| Subscriber Identity Module (SIM): |
| Wireless Two-Way Email |

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

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

|  |  |
| --- | --- |
| Cybersecurity Implementation Controls | Implementation Status |
| Identification Credentials |  |
| ID Card Scanning | Present |
| Biometric Login | Present |
| Password-based Login | Present |
| Digital Certificates using Cryptography | Absent |
| Government ID unique numbers | Absent |
| Personal Authentication |  |
| ID Card Scanning | Present |
| Biometric Login | Present |
| Password-based Login | Present |
| Digital Certificates using Cryptography | Absent |
| Government ID unique numbers | Absent |
| Authorization |  |
| Control Lists | Absent |
| Security Policies | Present |
| Use of Security Tokens | Present |
| Logical Access Controls Methods |  |
| Network Architecture Controls | Present |
| Remote Network Access | Present |
| Securing Network Ports | Absent |
| Logical Network Port Security | Absent |
| Port Authentication Using 802.1X | Absent |
| Encryption | Present |
| PKI Compliance Requirements | Absent |
| Passwords, PINs, and Implementations | Present |
| The DOD Common Access Card | Absent |
| Alternate Login Token | Present |
| Physical Access Control Methods |  |
| Classified Storage and Handling | Present |
| Attended Access | Absent |
| Access Points | Present |
| Smart Cards | Present |
| Physical Intrusion Detection Systems | Absent |
| PINs | Present |
| Physical Tokens | Absent |
| Biometric Systems |  |
| Fingerprint Scanners | Present |
| Eye Scanners | Absent |

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

|  |  |
| --- | --- |
| Cybersecurity Implementation Controls | Implementation Status |
| **Enclave Protection** |  |
| Defense-in-depth | Present |
| Use of Firewalls | Present |
| Use of Routers | Present |
| Use of Intrusion Detection System | Absent |
| Use of DMZ | Present |
| Use of VPN | Present |
| Use of Network Test Access Ports | Absent |
| **Firewalls** |  |
| Packet Filtering | Present |
| Screened Host | Absent |
| Stateful Inspection Firewall | Present |
| Application Proxy Gateway | Present |
| Hybrid Technology Firewall | Absent |
| **Routers** |  |
| Route Table Integrity | Present |
| Securing Routing Planes | Absent |

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

|  |  |
| --- | --- |
| Cybersecurity Implementation Controls | Implementation Status |
| **Ports, Protocols, and Services** |  |
| Different levels of blocking protocols at the enclave perimeter | Present |
| IPV4 Address Filtering | Present |
| IPV6 Address Filtering | Absent |
| Unicast Reverse Path Forwarding | Absent |
| Protecting Servers or LANS against SYN Flood Attack | Present |
| Blocking ICMPv4 echo request - echo reply and Traceroute utility | Present |
| **Device Management** |  |
| Vulnerability Management System | Present |
| Out-Of-Band Management | Absent |
| In-Band-Management | Present |
| **Device Monitoring** |  |
| Simple Network Management Protocol (SNMP) | Present |
| Network Management Station | Absent |
| **Network Authentication, Authorization and Accounting** |  |
| Authentication | Present |
| Authorization | Present |
| Accounting | Present |
| Auditing | Present |
| Routing Password Protection | Present |
| **Network Intrusion Detection Systems (NIDS)** |  |
| Local Area Network Intrusion Detection | Present |
| External Network Intrusion Detection | Absent |
| **Switches and VLANs** |  |
| Physical Switches and Wiring | Present |
| Virtual Local Area Networks (VLANs) | Present |
| VLAN Trunking | Present |
| VLAN Port Security | Absent |
| VLAN 802.1x and Management Policy Server | Absent |
| **Virtual Private Network** |  |
| Gateway-to-Gateway | Absent |
| Host-to-Gateway | Present |
| Host-to-Host | Absent |

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

|  |  |
| --- | --- |
| Cybersecurity Implementation Controls | Implementation Status |
| **Authentication** |  |
| Database User Accounts | Present |
| Database Administrator | Present |
| Application Owner | Present |
| Application User manager | Absent |
| Application Account | Absent |
| Database Auditor | Absent |
| Database Operator | Present |
| Passwords | Present |
| Certificates | Present |
| External Authentication | Present |
| Credential Storage | Present |
| **Authorization** |  |
| Access based on role | Present |
| Renaming default accounts | Absent |
| **Confidentiality** |  |
| Data file encryption | Present |
| Data encryption | Present |
| Source code encryption | Absent |
| **Data Integrity** |  |
| Transaction Logging | Present |
| Transaction Journaling | Present |
| **Auditing** |  |
| Audit Log Protection | Present |
| Audit Log Retention | Absent |
| Audit Reporting | Present |
| **Replication and Federation** |  |
| Database Replication | Present |
| Federated database | Absent |
| **Database Clustering** |  |
| Database Clustering | Present |
| Trial of accountability | Absent |
| Protection of Communication Path | Present |
| **Backup and Recovery** |  |
| Database backup and recovery testing | Present |
| Backup data encryption | Present |
| Access control for backup data | Present |
| **Operating System Protections** |  |
| Dedicated directories and files | Absent |
| Dedicated OS accounts | Present |
| Updated software | Present |
| **Application Protections** |  |
| Audit access to sensitive data | Present |
| Input validation | Present |
| Requirement for Authentication | Present |
| Avoiding display of unauthorized information | Absent |
| **Network Protections** |  |
| Giving access to users having requirement | Present |
| Restricting access to users | Present |
| Limits on network session parameters | Present |
| **Database Security design and Configuration** |  |
| Procedural Review | Present |
| Configuration Specification | Present |
| Compliance Testing | Present |
| Functional Architecture | Present |
| Non-repudiation | Present |
| Partitioning the Application | Absent |
| Configuration Management Process | Absent |
| IA Documentation | Absent |
| System Library Management Controls | Present |
| Security Support Structure Partitioning | Present |
| System State Changes | Present |
| Software Baseline | Absent |
| Individual Identification and Authentication | Present |
| Token and Certificate Standards | Present |
| **Enclave and Computing Environment** |  |
| Access for Need–to–know | Present |
| Audit Record Content | Present |
| Audit Trail, Monitoring, Analysis, and Reporting | Present |
| Changes to Data | Present |
| Encryption for data at rest | Present |
| Encryption for data in transit | Present |
| Data Change Controls | Present |
| Logon | Present |
| Audit of Security Label Changes | Present |
| Least Privilege | Absent |
| Marking and Labeling | Absent |
| Production Code Change Controls | Absent |
| Resource Control | Present |
| Audit Record Retention | Present |
| Security Configuration Compliance | Present |
| Warning Message | Absent |
| Boundary Defense | Present |
| Remote Access for Privileged Functions | Present |
| **Business Continuity** |  |
| Protection of Backup and Restoration Assets | Present |
| Data Backup Procedures | Present |
| Disaster and Recovery Planning | Present |
| Backup Copies of Critical Software | Absent |
| Trusted Recovery | Absent |
| **Vulnerability Management** |  |
| Vulnerability Management | Present |

* + 1. **Applications Security Risk Management Implementation Controls and Policies**

|  |  |
| --- | --- |
| Cybersecurity Implementation Controls | Implementation Status |
| **Application Data Handling** |  |
| Database management system | Present |
| Data storage | Present |
| In-Memory data handling | Present |
| Data Transmission | Present |
| Data Integrity | Present |
| Data Marking | Absent |
| **Authentication** |  |
| Server Authentication | Present |
| User Authentication | Present |
| Signed Code Identification | Present |
| Standalone Application Authentication | Absent |
| Server Application Authentication | Absent |
| Client Application Authentication | Present |
| Combination Client Server Application Authentication | Present |
| Application Component Authentication | Present |
| PKI Certificate Validation | Present |
| Password Complexity and Maintenance | Absent |
| Authentication Credentials Protection | Present |
| **Cryptography** |  |
| Use of Symmetric Cyphers | Present |
| Use of Digital Signature | Present |
| Use of Message Authentication Codes | Absent |
| **User Accounts** |  |
| Mechanism to detect duplicate user accounts | Present |
| Account Locking | Present |
| Manual Unlock Policy | Absent |
| Application Sessions | Absent |
| Access Control | Present |
| **Input Validation** |  |
| Integer Overflow | Present |
| Format String Vulnerabilities | Present |
| Command Injection Vulnerabilities | Absent |
| Buffer Overflows | Present |
| Race Conditions | Absent |
| **Application Auditing** |  |
| Auditing all access to need-to-know information | Present |
| Protection of contents of audit trails | Present |
| **Configuration Management** |  |
| Software Configuration Management | Absent |
| Release Manager | Present |
| **Testing** |  |
| Test Plans and Procedures | Present |
| Automated Tools | Present |
| Web Applications Vulnerability Scanners | Absent |
| **Deployment** |  |
| Documentation | Present |
| Maintenance and Availability | Present |
| Auditing | Absent |

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

|  |  |
| --- | --- |
| Cybersecurity Implementation Controls | Implementation Status |
| **Application Data Handling** |  |
| Database management system | Present |
| Data storage | Present |
| In-Memory data handling | Present |
| Data Transmission | Present |
| Data Integrity | Present |
| Data Marking | Absent |
| **Authentication** |  |
| Server Authentication | Present |
| User Authentication | Present |
| Signed Code Identification | Present |
| Standalone Application Authentication | Absent |
| Server Application Authentication | Absent |
| Client Application Authentication | Present |
| Combination Client Server Application Authentication | Present |
| Application Component Authentication | Present |
| PKI Certificate Validation | Present |
| Password Complexity and Maintenance | Absent |
| Authentication Credentials Protection | Present |
| **Cryptography** |  |
| Use of Symmetric Cyphers | Present |
| Use of Digital Signature | Present |
| Use of Message Authentication Codes | Absent |
| **User Accounts** |  |
| Mechanism to detect duplicate user accounts | Present |
| Account Locking | Present |
| Manual Unlock Policy | Absent |
| Application Sessions | Absent |
| Access Control | Present |
| **Input Validation** |  |
| Integer Overflow | Present |
| Format String Vulnerabilities | Present |
| Command Injection Vulnerabilities | Absent |
| Buffer Overflows | Present |
| Race Conditions | Absent |
| **Application Auditing** |  |
| Auditing all access to need-to-know information | Present |
| Protection of contents of audit trails | Present |
| **Configuration Management** |  |
| Software Configuration Management | Absent |
| Release Manager | Present |
| **Testing** |  |
| Test Plans and Procedures | Present |
| Automated Tools | Present |
| Web Applications Vulnerability Scanners | Absent |
| **Deployment** |  |
| Documentation | Present |
| Maintenance and Availability | Present |
| Auditing | Absent |

**List of Critical Assets that exist in Kshemin Innovations PVT LTD**

|  |  |  |
| --- | --- | --- |
| Asset No. | Asset Name | Asset Value |
| A1 | Personal Information | $25000 |
| A2 | Business Documents | $40000 |
| A3 | Hardware Components and Infrastructure | $30000 |
| A4 | Computers and network elements | $35000 |
| A5 | Storage elements, cloud services | $20000 |

**List of Potential Vulnerabilities at Kshemin Innovations PVT LTD**

* Easy Access
* Information Theft
* Unauthorized Access
* Access to Confidential Information
* Easy chance of exploitation
* Easy availability of an access point
* Insider Access

**List of Potential Threats at Kshemin Innovations PVT LTD**

* Hacking of Potential Systems
* Exposing Crucial Information
* Halt in Operations
* Irrecoverable damage to assets
* Loss of data

**List of Potential Risks at Kshemin Innovations PVT LTD**

* + Getting external access to systems
  + Access to unwanted cookies in the system
  + Detection of theft becomes difficult
  + Suspicious insider attack can take place
  + Identification of flaws within the security plan cannot take place
  + Loss in Confidentiality and Integrity

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

* To prevent unauthorized access, two-factor authentication must be introduced which will help solve the problem to some extent.
* Proper storage must be given to the information by using the cloud services, hard disks, multiple computers to solve the problem of data loss.
* Proper safety must be followed during power-off time and data transfer time.
* Proper anti-virus must be installed in company computers to protect systems from unauthorized access and data modification.
* Security controls and policies must be considered and implemented until a required level to control the complexity.
* Proper routing configuration should be set up to understand a clear way of incoming and outgoing data packets.
* Firewall should be implemented with the requirements of the institution by keeping in mind ports and protocols.
* DMZ must be implemented to keep less important services to protect the important assets.
* VPN service must be enabled to provide safe networking with people at long distances.
* Proper port scanning must be enabled to monitor the traffic of data flow.
* Out of band and in-band management should be set up to keep the working of applications in place.
* SNMP must be implemented well for an organized working environment in the company.
* Cryptographic methods must be used to protect every form of data, code, and files.
* Warning messages must be sent or printed if there is any slight modification of the existing data.
* Proper authentication techniques must be used for giving access to the database.
* Role-based authorization must be provided, and auditing of the files must be done.
* Network and Operating system must be checked from time to time, and it should be verified that there is no single access point for the outsiders.
* Role-based authorization must be provided, and auditing of the files must be done.
* IEEE standards and protocols must be followed strictly to ensure good security.
* Connectivity with Bluetooth and Wi-Fi must be verified as there can be open malicious networks.

**List of recommended Hardening Response controls and Policies for each recommended control that should be created to reduce risk impact and thus mitigate the identified risks and increase resilience – Risk Response Strategy**

* Company must make sure that all the business activities should not get stopped and work as per the regular schedule.
* Problem should be identified and should be analyzed by technological – management – operational teams.
* Proper response should be given to government regarding the attack so that the company can get some help.
* Operations from the compromised systems must be stopped and replaced with new or backup systems to decrease the loss of the attack.
* The vulnerabilities regarding networks must be scanned after an attack and actions must be taken to implement hardware or software assistance.
* Defense – in – depth mechanism must provide layered security in case of a data breach.
* It must be ensured that a threat agent must not exploit other assets even though the network is compromised.
* Important data must be stored in alternative hard drives and cloud services to protect in time of an attack.
* Software code and applications must be verified whether they are modified, and they must be immediately restored to the previous version.
* The source of the problem must be identified whether it occurred from the network, OS or Software, and that particular vulnerability must be resolved.
* Updating software, cryptographic methods, and checking audit logs must be done from time to time.

**Applicable Government Regulations and Industry Standards**

**Sarbanes-Oxley Act:**

It is a law framed to protect investors from fraudulent financial reporting by corporate organizations. The act created strict new rules for accountants, auditors, and corporate officers and imposed more stringent recordkeeping requirements. The act also added new criminal penalties for violating security laws. Corporates tend to modify their financial reports to protect themselves from tax payments. This law mainly addresses those issues. This law explains its concept through three sections namely Section 302, Section 404, and Section 802. 302 mandates that senior corporate officers personally certify the financial reports and are responsible for the truth in them. 404 mentions that management and auditors establish internal controls and reporting methods to ensure the adequacy of those controls. 802 mentions rules regarding recordkeeping. These deal with the falsification of records and electronic communications. Hence, this law plays an important role in protecting from submitting false financial records.

**Gramm-Leach-Bliley Act**:

It is a United States federal law requiring financial institutions to explain how they share and protect their customers’ nonpublic personal information (NPI). This mainly includes three rules namely The Financial Privacy Rule, The Safeguard Rule, and Pretexting Protection. The Financial Privacy Rule restricts the sharing of nonpublic personal information about an individual and ensures that every consumer is provided with a privacy note at the start. Data safeguard ensures that the financial institutions to develop an information security plan to protect customer’s data. Measures are taken to protect attacks like social engineering by providing pretexting protection.

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

It is Unites States federal law that defines a framework to safeguard federal data, operations and assets against threats. The act requires each federal agency to develop, document and implement a company-wide information security program to protect sensitive data and information systems. FISMA mainly advices to classify information as it is created, encrypt sensitive data, maintain evidence of FISMA compliance and stay up to date with the updates. FISMA assigned specific roles and responsibilities to federal agencies, NIST, and OMB to strengthen information security systems. After implementation, they must conduct an annual review and submit the results to the OMB. The OMB then utilizes the data to prepare the next updates in the annual implementation plan.

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

|  |  |  |
| --- | --- | --- |
| Domain | Top 5 Asset Risks | Top 5 Asset Vulnerabilities |
| Access Control | False Authentication can be possible | Easy Access |
| Modification of data and injection of virus into systems. | Information Theft |
| The weak access points in the network will be known and can be used later to enter the systems | Unauthorized Access |
| Authentication of a fake individual can be possible | Access to Confidential Information |
| No guarantee that the sender is sending the information | Improper Storage and Backup |
| Network Infrastructure | Getting external access to systems | Easy Access |
| Improper organization of data packets | Information Theft |
| Improper routing of data packets | Unauthorized Access |
| Access to unwanted cookies in the system | Access to Confidential Information |
| Possible DOS attack | Firewall Setting |
| Network Infrastructure Management | Getting external access into systems | Easy Access |
| Violation of unused ports and protocols | Information Theft |
| Possible DOS attack | Unauthorized Access |
| Lack of timed out option will expose the resources | Access to Confidential Information |
| Allowing access through improper address filtering | Firewall Setting |
| Database | Getting external access into systems | Easy Access |
| Detection of theft becomes difficult | Information Theft |
| Suspicious insider attack can take place | Unauthorized Access |
| Identification of flaws within the security plan cannot take place | Adding malware patch to the software |
| Trust in business with clients will be lost | Exposing key information |
| Application | Getting external access to systems | Easy Access |
| Detection of theft becomes difficult | Information Theft |
| Suspicious insider attack can take place | Unauthorized Access |
| Password cracking becomes easy by brute force | System crashing |
| A system crash can take place | Insider Access |
| Wireless | Getting external access to systems | Easy Access |
| Detection of theft becomes difficult | Information Theft |
| Suspicious insider attack can take place | Unauthorized Access |
| Identification of flaws within the security plan cannot take place | Access to Confidential Information |
| Loss in Confidentiality and Integrity | Easy chance of exploitation |

**List of Top 5 Risks:**

* Getting external access to systems
* Suspicious insider attack can take place
* The weak access points in the network will be known and can be used later to enter the systems
* Violation of unused ports and protocols
* A system crash can take place

**List of Top 5 Potential Vulnerabilities:**

* Unauthorized Access
* Firewall Setting
* Adding malware patch to the software
* Exposing key information
* Improper Storage and Backup

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

* To prevent unauthorized access, two-factor authentication must be introduced which will help solve the problem to some extent.
* Proper storage must be given to the information by using the cloud services, hard disks, multiple computers to solve the problem of data loss.
* Proper safety must be followed during power-off time and data transfer time.
* Proper anti-virus must be installed in company computers to protect systems from unauthorized access and data modification.
* Security controls and policies must be considered and implemented until a required level to control the complexity.
* Proper routing configuration should be set up to understand a clear way of incoming and outgoing data packets.
* Firewall should be implemented with the requirements of the institution by keeping in mind ports and protocols.
* DMZ must be implemented to keep less important services to protect the important assets.
* VPN service must be enabled to provide safe networking with people at long distances.
* Proper port scanning must be enabled to monitor the traffic of data flow.
* Out of band and in-band management should be set up to keep the working of applications in place.
* SNMP must be implemented well for an organized working environment in the company.
* Cryptographic methods must be used to protect every form of data, code, and files.
* Warning messages must be sent or printed if there is any slight modification of the existing data.
* Proper authentication techniques must be used for giving access to the database.
* Role-based authorization must be provided, and auditing of the files must be done.
* Network and Operating system must be checked from time to time, and it should be verified that there is no single access point for the outsiders.
* Role-based authorization must be provided, and auditing of the files must be done.
* IEEE standards and protocols must be followed strictly to ensure good security.
* Connectivity with Bluetooth and Wi-Fi must be verified as there can be open malicious networks.

**List of recommended Hardening Response controls and Policies for each recommended control that should be created to reduce risk impact and thus mitigate the identified risks and increase resilience – Risk Response Strategy**

* Company must make sure that all the business activities should not get stopped and work as per the regular schedule.
* Problem should be identified and should be analyzed by technological – management – operational teams.
* Proper response should be given to government regarding the attack so that the company can get some help.
* Operations from the compromised systems must be stopped and replaced with new or backup systems to decrease the loss of the attack.
* The vulnerabilities regarding networks must be scanned after an attack and actions must be taken to implement hardware or software assistance.
* Defense – in – depth mechanism must provide layered security in case of a data breach.
* It must be ensured that a threat agent must not exploit other assets even though the network is compromised.
* Important data must be stored in alternative hard drives and cloud services to protect in time of an attack.
* Software code and applications must be verified whether they are modified, and they must be immediately restored to the previous version.
* The source of the problem must be identified whether it occurred from the network, OS or Software, and that particular vulnerability must be resolved.
* Updating software, cryptographic methods, and checking audit logs must be done from time to time.

**Cybersecurity Workforce Risk Management Implementation**

**List of cybersecurity Speciality Areas that exist at Kshemin Innovations PVT LTD**

|  |
| --- |
| Risk Management (RSK) |
| Software Development (DEV) |
| Systems Architecture (ARC) |
| Test and Evaluation (TST) |
| Systems Development (SYS) |
| Data Administration (DTA) |
| Network Services (NET) |
| Training, Education, and Awareness (TEA) |
| Cybersecurity Management (MGT) |
| Strategic Planning and Policy (SPP) |
| Cybersecurity Defense Analysis (CDA) |
| Incident Response (CIR) |
| Vulnerability Assessment and Management (VAM) |
| Threat Analysis (TWA) |
| Cyber Investigation (INV) |

**List of cybersecurity Work Roles that exist at Kshemin Innovations PVT LTD**

|  |
| --- |
| Authorizing Official/ Designating Representative |
| Security Control Assessor |
| Software Developer |
| Secure Software Assessor |
| Enterprise Architect |
| Security Architect |
| System Testing and Evaluation Specialist |
| Works on the development phases of the systems development life cycle. |
| Database Administrator |
| Network Operations Specialist |
| Cyber Instructional Curriculum Developer |
| Information Systems Security Manager |
| Cyber Policy and Strategy Planner |
| Cyber Defense Analyst |
| Cyber Defense Incident Responder |
| Vulnerability Assessment Analyst |
| Cyber Crime Investigator |

**List of cybersecurity Tasks that exists at Kshemin Innovations PVT LTD**

|  |
| --- |
| 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. |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). |
| Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). |
| Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks. |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. |
| 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. |
| Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application. |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. |
| Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. |
| Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements. |
| Develop software system testing and validation procedures, programming, and documentation. |
| Develop threat model based on customer interviews and requirements. |
| Consult with engineering staff to evaluate interface between hardware and software. |
| Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. |
| Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct. |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. |
| Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. |
| Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. |
| Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). |
| Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements. |
| Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. |
| Develop and direct system testing and validation procedures and documentation. |
| Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. |
| Analyze and plan for anticipated changes in data capacity requirements. |
| Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing. |
| Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems. |
| Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling). |
| Diagnose network connectivity problem. |
| Install or replace network hubs, routers, and switches. |
| Monitor network capacity and performance. |
| Test and maintain network infrastructure including software and hardware devices. |
| 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. |
| 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. |
| Ensure that security improvement actions are evaluated, validated, and implemented as required. |
| Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. |
| Review existing and proposed policies with stakeholders. |
| Define and integrate current and future mission environments. |
| Support the CIO in the formulation of cyber-related policies. |
| Develop content for cyber defense tools. |
| Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. |
| Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. |
| Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. |
| 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. |
| Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. |
| Conduct and/or support authorized penetration testing on enterprise network assets. |
| Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. |
| 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). |
| Provide subject matter expertise to the development of a common operational picture. |
| Maintain a common intelligence picture. |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. |
| Conduct in-depth research and analysis. |
| Develop information requirements necessary for answering priority information requests. |
| Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets. |
| Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations. |
| 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). |
| Identify elements of proof of the crime. |
| Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. |
| Provide criminal investigative support to trial counsel during the judicial process. |

**Comparison of the NCWF recommended Cybersecurity specialty Areas with Kshemin Innovations PVT LTD’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) | Absent |
| Test and Evaluation (TST) | Present |
| Systems Development (SYS) | Present |
| Data Administration (DTA) | Present |
| Knowledge Management (KMG) | Absent |
| Customer Service and Technical Support (STS) | Absent |
| Network Services (NET) | Present |
| System Administration (ADM) | Absent |
| System Analysis (ANA) | Absent |
| Legal Advice and Advocacy (LGA) | Absent |
| Training, Education, and Awareness (TEA) | Present |
| Cybersecurity Management (MGT) | Present |
| Strategic Planning and Policy (SPP) | Present |
| Executive Cyber Leadership (EXL) | Absent |
| Program/Project Management (PMA) and Acquisition | Absent |
| Cybersecurity Defense Analysis (CDA) | Present |
| Cybersecurity Defense Infrastructure Support (INF) | Absent |
| Incident Response (CIR) | Present |
| Vulnerability Assessment and Management (VAM) | Present |
| Threat Analysis (TWA) | Present |
| Exploitation Analysis (EXP) | Absent |
| All-Source Analysis (ASA) | Absent |
| Targets (TGT) | Absent |
| Language Analysis (LNG) | Absent |
| Collection Operations (CLO) | Absent |
| Cyber Operational Planning (OPL) | Absent |
| Cyber Operations (OPS) | Absent |
| Cyber Investigation (INV) | Present |
| Digital Forensics (FOR) | Absent |

**Comparison of the NCWF recommended Cybersecurity Work Roles with Kshemin Innovations PVT LTD’s existing Cybersecurity Work Roles and Comparison of the NCWF recommended Cybersecurity Tasks with Kshemin Innovations PVT LTD’s existing Cybersecurity Tasks**

|  |  |  |
| --- | --- | --- |
| **Work Role** | **Tasks** | **Status** |
| Authorizing Official/Designating Representative | Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). | Present |
| Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. | Present |
| Establish acceptable limits for the software application, network, or system. | Present |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). | Absent |
| Security Control Assessor | Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2). | Present |
| Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks. | Present |
| Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network. | Present |
| Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations. | Present |
| Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers). | Absent |
| Establish acceptable limits for the software application, network, or system. | Absent |
| Manage Accreditation Packages (e.g., ISO/IEC 15026-2). | Present |
| Perform security reviews, identify gaps in security architecture, and develop a security risk management plan. | Present |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. | Present |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Present |
| Verify and update security documentation reflecting the application/system security design features. | 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). | Present |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Present |
| Assess the effectiveness of security controls. | Present |
| Assess all the configuration management (change configuration/release management) processes. | Present |
| Software Developer | Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application. | Present |
| Analyze user needs and software requirements to determine feasibility of design within time and cost constraints. | Present |
| Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. | Present |
| Apply secure code documentation. | Present |
| Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules. | Present |
| Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program. | Present |
| Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces. | Present |
| Consult with engineering staff to evaluate interface between hardware and software. | Absent |
| 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. | Present |
| Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. | Present |
| Identify basic common coding flaws at a high level. | Present |
| Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise’s computer systems in software development. | Present |
| Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life. | Present |
| Perform integrated quality assurance testing for security functionality and resiliency attack. | Present |
| Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities. | Present |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Present |
| Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language. | Present |
| Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. | Present |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | 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. | Present |
| Consult with customers about software system design and maintenance. | Present |
| Direct software programming and development of documentation. | Present |
| Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Present |
| Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate. | Present |
| Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate. | Present |
| Secure Software Assessor | Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews. | Present |
| Apply secure code documentation. | Present |
| Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules. | Present |
| Develop threat model based on customer interviews and requirements. | Present |
| Consult with engineering staff to evaluate interface between hardware and software. | Present |
| Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration. | Present |
| Identify basic common coding flaws at a high level. | 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. | 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. | Present |
| Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing. | Present |
| Store, retrieve, and manipulate data for analysis of system capabilities and requirements. | Present |
| Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria. | Present |
| Perform penetration testing as required for new or updated applications. | Present |
| Consult with customers about software system design and maintenance. | Present |
| Direct software programming and development of documentation. | Present |
| Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel. | Present |
| Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application. | Present |
| Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates. | Present |
| Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct. | Present |
| Develop secure software testing and validation procedures. | Absent |
| Develop system testing and validation procedures, programming, and documentation. | Absent |
| Enterprise Architect | Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | Present |
| Employ secure configuration management processes. | Present |
| Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. | Present |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. | Present |
| Provide advice on project costs, design concepts, or design changes. | Present |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | Present |
| Analyze candidate architectures, allocate security services, and select security mechanisms. | Present |
| Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements. | Present |
| Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents. | Present |
| Write detailed functional specifications that document the architecture development process. | Present |
| Analyze user needs and requirements to plan architecture. | 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. | Present |
| 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. | Present |
| Translate proposed capabilities into technical requirements. | Absent |
| Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture. | Absent |
| Integrate key management functions as related to cyberspace. | Absent |
| Security Architect | Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event. | Present |
| Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration. | 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. | Present |
| Employ secure configuration management processes. | Present |
| Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines. | Present |
| Identify and prioritize critical business functions in collaboration with organizational stakeholders. | Present |
| 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. | Present |
| Provide input on security requirements to be included in statements of work and other appropriate procurement documents. | Present |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle 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. | Present |
| Write detailed functional specifications that document the architecture development process. | Present |
| Analyze user needs and requirements to plan architecture. | Present |
| Develop enterprise architecture or system components required to meet user needs. | Present |
| Document and update as necessary all definition and architecture activities. | Present |
| Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately. | Present |
| Translate proposed capabilities into technical requirements. | Present |
| Assess and design security management functions as related to cyberspace. | Present |
| Research & Development Specialist | Review and validate data mining and data warehousing programs, processes, and requirements. | Absent |
| Research current technology to understand capabilities of required system or network. | Absent |
| Identify cyber capabilities strategies for custom hardware and software development based on mission requirements. | Absent |
| Collaborate with stakeholders to identify and/or develop appropriate solutions technology. | Absent |
| Design and develop new tools/technologies as related to cybersecurity. | Absent |
| Evaluate network infrastructure vulnerabilities to enhance capabilities being developed. | Absent |
| Follow software and systems engineering life cycle standards and processes. | Absent |
| Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases. | Absent |
| Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities. | Absent |
| Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. | Absent |
| Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce. | Absent |
| Research and evaluate available technologies and standards to meet customer requirements. | Absent |
| Systems Requirements Planner | Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications. | Absent |
| Consult with customers to evaluate functional requirements. | Absent |
| Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions. | Absent |
| Define project scope and objectives based on customer requirements. | Absent |
| Develop and document requirements, capabilities, and constraints for design procedures and processes. | Absent |
| Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements. | 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. | Absent |
| Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware). | Absent |
| Define baseline security requirements in accordance with applicable guidelines. | Absent |
| Develop cost estimates for new or modified system(s). | Absent |
| System Testing and Evaluation Specialist | Determine level of assurance of developed capabilities based on test results. | Present |
| Develop test plans to address specifications and requirements. | Present |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Present |
| Make recommendations based on test results. | Present |
| Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated. | Present |
| Create auditable evidence of security measures. | Present |
| Validate specifications and requirements for testability. | Present |
| Analyze the results of software, hardware, or interoperability testing. | Present |
| Perform developmental testing on systems under development. | Present |
| Perform interoperability testing on systems exchanging electronic information with other systems. | Present |
| Perform operational testing. | Present |
| Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements. | Present |
| Record and manage test data. | Present |
| Information Systems Security Developer | 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. | Absent |
| Assess the effectiveness of cybersecurity measures utilized by system(s). | Absent |
| Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile. | Absent |
| Build, test, and modify product prototypes using working models or theoretical models. | Present |
| 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. | Present |
| Develop and direct system testing and validation procedures and documentation. | Absent |
| Develop detailed security design documentation for component and interface specifications to support system design and development. | Absent |
| Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment. | Absent |
| Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed. | Absent |
| Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications. | Absent |
| Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements. | Absent |
| Systems Developer | Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support. | Present |
| Build, test, and modify product prototypes using working models or theoretical models. | Present |
| Design and develop cybersecurity or cybersecurity-enabled products. | 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. | Present |
| Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change. | Absent |
| Provide guidelines for implementing developed systems to customers or installation teams. | Absent |
| Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials). | 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 |
| Database Administrator | Analyze and plan for anticipated changes in data capacity requirements. | Present |
| Maintain database management systems software. | Present |
| Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing. | Present |
| Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required. | Present |
| Manage the compilation, cataloging, caching, distribution, and retrieval of data. | Present |
| Monitor and maintain databases to ensure optimal performance. | Present |
| Perform backup and recovery of databases to ensure data integrity. | Present |
| Provide recommendations on new database technologies and architectures. | Present |
| Performs configuration management, problem management, capacity management, and financial management for databases and data management systems. | Present |
| Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems. | Absent |
| Data Analyst | Analyze and define data requirements and specifications. | Present |
| Analyze and plan for anticipated changes in data capacity requirements. | Present |
| Develop data standards, policies, and procedures. | Present |
| Manage the compilation, cataloging, caching, distribution, and retrieval of data. | Present |
| Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements. | Present |
| Provide recommendations on new database technologies and architectures. | Absent |
| Analyze data sources to provide actionable recommendations. | Absent |
| Assess the validity of source data and subsequent findings. | Present |
| Collect metrics and trending data. | Present |
| Conduct hypothesis testing using statistical processes. | Present |
| Confer with systems analysts, engineers, programmers, and others to design application. | Present |
| Develop and facilitate data-gathering methods. | Absent |
| Develop strategic insights from large data sets. | Absent |
| Present technical information to technical and nontechnical audiences. | Present |
| Present data in creative formats. | Present |
| Knowledge Manager | Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users. | Absent |
| Develop an understanding of the needs and requirements of information end-users. | Absent |
| Monitor and report the usage of knowledge management assets and resources. | Absent |
| Plan and manage the delivery of knowledge management projects. | Absent |
| Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information. | Absent |
| Lead efforts to promote the organization's use of knowledge management and information sharing. | Absent |
| Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files). | Absent |
| Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization’s intellectual capital. | Absent |
| Technical Support Specialist | Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Absent |
| Troubleshoot system hardware and software. | Absent |
| Analyze incident data for emerging trends. | Absent |
| Develop and deliver technical training to educate others or meet customer needs. | Absent |
| 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. | Absent |
| Perform asset management/inventory of information technology (IT) resources. | Absent |
| Network Operations Specialist | Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling). | Present |
| Develop and implement network backup and recovery procedures. | Present |
| Diagnose network connectivity problem. | Present |
| Implement new system design procedures, test procedures, and quality standards. | Present |
| Install and maintain network infrastructure device operating system software (e.g., IOS, firmware). | Present |
| Install or replace network hubs, routers, and switches. | Absent |
| Integrate new systems into existing network architecture. | Absent |
| Monitor network capacity and performance. | Absent |
| Patch network vulnerabilities to ensure that information is safeguarded against outside parties. | Present |
| Provide feedback on network requirements, including network architecture and infrastructure. | Present |
| System Administrator | 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 |
| Systems Security Analyst | 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 |
| Cyber Legal Advisor | Advocate organization's official position in legal and legislative proceedings. | Absent |
| Evaluate contracts to ensure compliance with funding, legal, and program requirements. | Absent |
| Evaluate the effectiveness of laws, regulations, policies, standards, or procedures. | Absent |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances. | Present |
| Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance. | Present |
| 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 |
| Privacy Officer/Privacy Compliance Manager | Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. | Absent |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| Conduct functional and connectivity testing to ensure continuing operability. | Absent |
| Establish a risk management strategy for the organization that includes a determination of risk tolerance. | Absent |
| Conduct Privacy Impact Assessments (PIAs) of the application’s security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII). | 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. | Present |
| Interpret and apply laws, regulations, policies, standards, or procedures to specific issues. | Absent |
| Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise’s cybersecurity program. | Absent |
| Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. | Absent |
| Present technical information to technical and nontechnical audiences. | Absent |
| Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. | Absent |
| Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients. | Absent |
| Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations. | Absent |
| Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements. | Absent |
| Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner. | Present |
| Liaise with regulatory and accrediting bodies. | Present |
| 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 |
| Cyber Instructional Curriculum Developer | Support the design and execution of exercise scenarios. | Present |
| Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. | Present |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. | Present |
| Research current technology to understand capabilities of required system or network. | Present |
| Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction. | Present |
| Conduct learning needs assessments and identify requirements. | Present |
| Create interactive learning exercises to create an effective learning environment. | Present |
| Develop or assist in the development of training policies and protocols for cyber training. | Present |
| Develop the goals and objectives for cyber curriculum. | Present |
| Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers. | Present |
| Correlate training and learning to business or mission requirements. | Absent |
| Create training courses tailored to the audience and physical environment. | Absent |
| Cyber Instructor | Conduct interactive training exercises to create an effective learning environment. | Absent |
| Develop new or identify existing awareness and training materials that are appropriate for intended audiences. | Absent |
| Evaluate the effectiveness and comprehensiveness of existing training programs. | Absent |
| Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions). | Absent |
| Support the design and execution of exercise scenarios. | Absent |
| Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce. | Absent |
| Develop or assist in the development of computer based training modules or classes. | Absent |
| Develop or assist in the development of course assignments. | Absent |
| Develop or assist in the development of course evaluations. | Absent |
| Develop or assist in the development of grading and proficiency standards. | Absent |
| Assist in the development of individual/collective development, training, and/or remediation plans. | Present |
| Develop or assist in the development of learning objectives and goals. | Present |
| Information Systems Security Manager | Manage the monitoring of information security data sources to maintain organizational situational awareness. | Present |
| Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency. | Present |
| Manage threat or target analysis of cyber defense information and production of threat information within the enterprise. | Present |
| Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection. | Present |
| Oversee the information security training and awareness program. | Present |
| Participate in an information security risk assessment during the Security Assessment and Authorization process. | Present |
| Participate in the development or modification of the computer environment cybersecurity program plans and requirements. | Present |
| Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations. | Present |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | 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. | Present |
| Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents. | Present |
| Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters. | Present |
| Recognize a possible security violation and take appropriate action to report the incident, as required. | Present |
| Recommend resource allocations required to securely operate and maintain an organization’s cybersecurity requirements. | Present |
| Recommend policy and coordinate review and approval. | Present |
| Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered. | Present |
| Track audit findings and recommendations to ensure that appropriate mitigation actions are taken. | Present |
| Use federal and organization-specific published documents to manage operations of their computing environment system(s). | Present |
| Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals. | Absent |
| Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies. | Present |
| Communications Security (COMSEC) Manager | Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture. | Absent |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| 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 |
| Cyber Workforce Developer and Manager | Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. | Absent |
| Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements. | Absent |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Absent |
| Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance. | Present |
| Develop policy, programs, and guidelines for implementation. | Present |
| Establish and maintain communication channels with stakeholders. | Present |
| Evaluate cost/benefit, economic, and risk analysis in decision-making process. | Absent |
| Identify organizational policy stakeholders. | Absent |
| Review existing and proposed policies with stakeholders. | Absent |
| Serve on agency and interagency policy boards. | Absent |
| Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. | Present |
| 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. | Absent |
| Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets. | Present |
| 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 |
| Cyber Policy and Strategy Planner | Develop policy, programs, and guidelines for implementation. | Present |
| Establish and maintain communication channels with stakeholders. | Present |
| Review existing and proposed policies with stakeholders. | Present |
| Serve on agency and interagency policy boards. | Present |
| Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials. | Present |
| Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices. | Absent |
| Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals. | Present |
| Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards. | Present |
| Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy. | Present |
| Analyze organizational cyber policy. | Present |
| Executive Cyber Leadership | Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk. | Present |
| Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program. | Present |
| 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. | Present |
| Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders. | Absent |
| Develop and maintain strategic plans. | Absent |
| Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network 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. | Present |
| 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 |
| Program Manager | 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. | Absent |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | Absent |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| Review or conduct audits of information technology (IT) programs and projects. | Present |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Absent |
| Develop and document supply chain risks for critical system elements, as appropriate. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Absent |
| IT Project Manager | Develop methods to monitor and measure risk, compliance, and assurance efforts. | Absent |
| Perform needs analysis to determine opportunities for new and improved business process solutions. | Absent |
| Provide advice on project costs, design concepts, or design changes. | Absent |
| Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans. | Absent |
| Provide ongoing optimization and problem-solving support. | Present |
| 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 |
| Product Support Manager | Develop methods to monitor and measure risk, compliance, and assurance efforts. | Absent |
| Perform needs analysis to determine opportunities for new and improved business process solutions. | Absent |
| Provide advice on project costs, design concepts, or design changes. | Absent |
| Provide input to implementation plans and standard operating procedures. | Absent |
| Provide ongoing optimization and problem-solving support. | Present |
| Provide recommendations for possible improvements and upgrades. | Present |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| Review or conduct audits of information technology (IT) programs and projects. | 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. | Present |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Present |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Present |
| Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully. | Present |
| Coordinate and manage the overall service provided to a customer end-to-end. | 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 |
| IT Investment/Portfolio Manager | Resolve conflicts in laws, regulations, policies, standards, or procedures. | Absent |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals. | Absent |
| Develop contract language to ensure supply chain, system, network, and operational security are met. | Absent |
| Gather feedback on customer satisfaction and internal service performance to foster continual improvement. | Absent |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Present |
| Lead and oversee budget, staffing, and contracting. | Present |
| Draft and publish supply chain security and risk management documents. | Present |
| IT Program Auditor | Develop methods to monitor and measure risk, compliance, and assurance efforts. | Present |
| Provide ongoing optimization and problem-solving support. | Present |
| Provide recommendations for possible improvements and upgrades. | Present |
| Review or conduct audits of information technology (IT) programs and projects. | Absent |
| Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements. | Present |
| Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up. | Present |
| Conduct import/export reviews for acquiring systems and software. | Present |
| Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered. | Present |
| Cyber Defense Analyst | 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. | Absent |
| Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level. | Absent |
| Document and escalate incidents (including event’s history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment. | Present |
| Perform cyber defense trend analysis and reporting. | Present |
| Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack. | Present |
| Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy. | Present |
| Plan and recommend modifications or adjustments based on exercise results or system environment. | Present |
| Provide daily summary reports of network events and activity relevant to cyber defense practices. | Present |
| Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts. | Present |
| Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities. | Present |
| Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity. | Present |
| Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information. | Present |
| Determine tactics, techniques, and procedures (TTPs) for intrusion sets. | Present |
| Cyber Defense Infrastructure Support Specialist | Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications. | Present |
| 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. | Present |
| Build, install, configure, and test dedicated cyber defense hardware. | Absent |
| 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). | Absent |
| Cyber Defense Incident Responder | Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents. | Present |
| Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation. | Present |
| Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security. | Present |
| Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation. | Present |
| Perform cyber defense trend analysis and reporting. | Present |
| Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems. | Present |
| Perform real-time cyber 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. | Present |
| Track and document cyber defense incidents from initial detection through final resolution. | Present |
| Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies. | Present |
| Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness). | Present |
| Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise. | Present |
| Serve as technical expert and liaison to law enforcement personnel and explain incident details as required. | Absent |
| Coordinate with intelligence analysts to correlate threat assessment data. | Absent |
| Write and publish after action reviews. | Absent |
| Vulnerability Assessment Analyst | Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives. | Present |
| Conduct and/or support authorized penetration testing on enterprise network assets. | Present |
| Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions. | Present |
| Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing. | Present |
| Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions. | Present |
| Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews). | Present |
| Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications). | Present |
| Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes). | Absent |
| Threat/Warning Analyst | Answer requests for information. | Present |
| Provide subject matter expertise to the development of a common operational picture. | Present |
| Maintain a common intelligence picture. | Present |
| Provide subject matter expertise to the development of cyber operations specific indicators. | Present |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Present |
| Assist in the identification of intelligence collection shortfalls. | Present |
| 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. | Present |
| Develop information requirements necessary for answering priority information requests. | Present |
| Evaluate threat decision-making processes. | Present |
| Identify threats to Blue Force vulnerabilities. | Present |
| Generate requests for information. | Present |
| 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. | Absent |
| Exploitation Analyst | 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. | Present |
| Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements. | Present |
| Apply and obey applicable statutes, laws, regulations and policies. | Absent |
| Perform analysis for target infrastructure exploitation activities. | Absent |
| Collaborate with other internal and external partner organizations on target access and operational issues. | Absent |
| Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers. | Absent |
| Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access. | Absent |
| Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access. | Absent |
| Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities. | Absent |
| Examine intercept-related metadata and content with an understanding of targeting significance. | Absent |
| Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development. | Absent |
| Identify gaps in our understanding of target technology and developing innovative collection approaches. | Absent |
| Identify, locate, and track targets via geospatial analysis techniques. | Absent |
| Lead or enable exploitation operations in support of organization objectives and target requirements. | Absent |
| Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications. | Absent |
| All-Source Analyst | Answer requests for information. | Absent |
| Provide expertise to course of action development. | Absent |
| Provide subject matter expertise to the development of a common operational picture. | Absent |
| Maintain a common intelligence picture. | Absent |
| Provide subject matter expertise to the development of cyber operations specific indicators. | Absent |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Absent |
| Assist in the identification of intelligence collection shortfalls. | Absent |
| Brief threat and/or target current situations. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Conduct in-depth research and analysis. | Absent |
| Conduct nodal analysis. | Absent |
| Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology. | Absent |
| Develop information requirements necessary for answering priority information requests. | Absent |
| Engage customers to understand customers’ intelligence needs and wants. | Absent |
| Evaluate threat decision-making processes. | Absent |
| Identify threat vulnerabilities. | Absent |
| Identify threats to Blue Force vulnerabilities. | Absent |
| Generate requests for information. | Absent |
| Identify threat tactics, and methodologies. | Absent |
| Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. | Absent |
| Mission Assessment Specialist | Provide expertise to course of action development. | Absent |
| Provide subject matter expertise to the development of a common operational picture. | Absent |
| Provide subject matter expertise to the development of cyber operations specific indicators. | Absent |
| Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities. | Absent |
| Provide expertise to the development of measures of effectiveness and measures of performance. | Absent |
| Assist in the identification of intelligence collection shortfalls. | Absent |
| Brief threat and/or target current situations. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Conduct end-of-operations assessments. | Absent |
| Conduct in-depth research and analysis. | Absent |
| Conduct nodal analysis. | Absent |
| Conduct target research and analysis. | Absent |
| Develop information requirements necessary for answering priority information requests. | Absent |
| Develop measures of effectiveness and measures of performance. | Absent |
| Develop munitions effectiveness assessment or operational assessment materials. | Absent |
| Engage customers to understand customers’ intelligence needs and wants. | Absent |
| Estimate operational effects generated through cyber activities. | Absent |
| Evaluate threat decision-making processes. | Absent |
| Identify threat vulnerabilities. | Absent |
| Generate requests for information. | Absent |
| Target Developer | Accurately characterize targets. | Absent |
| Provide expertise to course of action development. | Absent |
| Provide expertise to the development of measures of effectiveness and measures of performance. | Absent |
| Build and maintain electronic target folders. | Absent |
| Collaborate with intelligence analysts/targeting organizations involved in related areas. | Absent |
| Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas. | Absent |
| Conduct nodal analysis. | Absent |
| Conduct target research and analysis. | Absent |
| Coordinate target vetting with appropriate partners. | Absent |
| Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology. | Absent |
| Determine what technologies are used by a given target. | Present |
| Develop all-source intelligence targeting materials. | Present |
| Develop measures of effectiveness and measures of performance. | Present |
| Develop munitions effectiveness assessment or operational assessment materials. | Present |
| Estimate operational effects generated through cyber activities. | Present |
| Evaluate available capabilities against desired effects to recommend efficient solutions. | Present |
| Generate requests for information. | Absent |
| Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. | Absent |
| Target Network Analyst | Provide expertise to course of action development. | Absent |
| Classify documents in accordance with classification guidelines. | Absent |
| Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas. | Absent |
| Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. | Absent |
| Identify and conduct analysis of target communications to identify information essential to support operations. | Absent |
| Conduct nodal analysis. | Absent |
| Conduct quality control to determine validity and relevance of information gathered about networks. | Absent |
| Conduct target research and analysis. | Absent |
| Determine what technologies are used by a given target. | Absent |
| Apply analytic techniques to gain more target information. | Absent |
| Generate and evaluate the effectiveness of network analysis strategies. | Absent |
| Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.) | Absent |
| Generate requests for information. | Absent |
| Identify and evaluate threat critical capabilities, requirements, and vulnerabilities. | Absent |
| Identify collection gaps and potential collection strategies against targets. | Absent |
| Multi-Disciplined Language Analyst | Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets. | Absent |
| Determine what technologies are used by a given target. | Absent |
| Identify collection gaps and potential collection strategies against targets. | Absent |
| Make recommendations to guide collection in support of customer requirements. | Absent |
| Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate. | Absent |
| Advise managers and operators on language and cultural issues that impact organization objectives. | Absent |
| 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. | Present |
| Conduct analysis of target communications to identify essential information in support of organization objectives. | Present |
| Perform quality review and provide feedback on transcribed or translated materials. | 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 |
| All Source-Collection Manager | 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 |
| All Source-Collection Requirements Manager | 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 |
| Cyber Intel Planner | Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives. | Absent |
| Coordinate for intelligence support to operational planning activities. | Absent |
| Assess all-source intelligence and recommend targets to support cyber operation objectives. | Absent |
| Assess target vulnerabilities and/or operational capabilities to determine course of action. | Absent |
| Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. | Absent |
| Assist in the development and refinement of priority information requirements. | Absent |
| Enable synchronization of intelligence support plans across partner organizations as required. | Absent |
| Provide input to the identification of cyber-related success criteria. | Absent |
| Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials). | Absent |
| Contribute to crisis action planning for cyber operations. | Absent |
| Contribute to the development of the organization's decision support tools if necessary. | Absent |
| Incorporate intelligence equities into the overall design of cyber operations plans. | Absent |
| Coordinate with intelligence planners to ensure that collection managers receive information requirements. | Absent |
| Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks. | Absent |
| Coordinate, produce, and track intelligence requirements. | Absent |
| Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans. | Absent |
| Use intelligence estimates to counter potential target actions. | Absent |
| Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives. | Absent |
| Develop and review intelligence guidance for integration into supporting cyber operations planning and execution. | Absent |
| Develop detailed intelligence support to cyber operations requirements. | Absent |
| Cyber Ops Planner | 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 |
| Partner Integration Planner | Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement. | Absent |
| Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives. | Absent |
| Provide expertise to course of action development. | Absent |
| Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials). | Absent |
| Contribute to crisis action planning for cyber operations. | Absent |
| Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers. | Absent |
| Coordinate with intelligence and cyber defense partners to obtain relevant essential information. | Present |
| Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations. | Present |
| Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives. | Present |
| 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. | Present |
| Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community. | Present |
| 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 |
| Cyber Operator | Analyze internal operational architecture, tools, and procedures for ways to improve performance. | Absent |
| Analyze target operational architecture for ways to gain access. | Absent |
| Collaborate with development organizations to create and deploy the tools needed to achieve objectives. | Absent |
| Conduct access enabling of wireless computer and digital networks. | Absent |
| Conduct collection and processing of wireless computer and digital networks. | Absent |
| Conduct exploitation of wireless computer and digital networks. | 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 |
| Cyber Crime Investigator | Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects. | Present |
| Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. | Present |
| Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals). | Present |
| Examine recovered data for information of relevance to the issue at hand. | Present |
| Fuse computer network attack analyses with criminal and counterintelligence investigations and operations. | Present |
| Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action. | Present |
| Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations. | Present |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. | Present |
| Identify elements of proof of the crime. | Present |
| Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations. | Present |
| Process crime scenes. | Present |
| Secure the electronic device or information source. | Present |
| Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence. | Present |
| Analyze the crisis to ensure public, personal, and resource protection. | Present |
| Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation. | Present |
| Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks. | Present |
| Provide criminal investigative support to trial counsel during the judicial process. | Present |
| Analyze computer-generated threats for counterintelligence or criminal activity. | Present |
| Gather and preserve evidence used on the prosecution of computer crimes. | Present |
| Law Enforcement /CounterIntelligence Forensics Analyst | 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 |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| Analyze incident data for emerging trends. | Present |
| Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis. | Present |
| Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, 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). | Present |
| Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities. | Present |
| Analyze organizational cyber policy. | Present |
| Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet. | Present |
| Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals). | Present |
| Resolve conflicts in laws, regulations, policies, standards, or procedures. | Present |
| Cyber Defense Forensics Analyst | 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. | Absent |
| Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats. | Absent |
| Decrypt seized data using technical means. | Absent |
| Provide technical summary of findings in accordance with established reporting procedures. | Absent |
| Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence. | Absent |
| Examine recovered data for information of relevance to the issue at hand. | Absent |
| Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration. | Absent |
| Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment. | Absent |
| Perform file signature analysis. | Absent |
| Perform hash comparison against established database. | Absent |
| Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView). | Absent |
| Perform timeline analysis. | Absent |
| Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs). | Absent |
| Perform static media analysis. | Absent |
| Perform tier 1, 2, and 3 malware analysis. | 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 |

**List of potential threats to Kshemin Innovations PVT LTD that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, work roles, and cybersecurity tasks.**

|  |
| --- |
| **Threats** |
| Hacking of Potential Systems |
| Exposing Crucial Information |
| Halt in Operations |
| Irrecoverable damage to assets |
| Loss of data |
| Application and database damage |
| Denial of Service |

**List of potential risks for critical assets where cybersecurity speciality areas, cybersecurity work roles, and cybersecurity tasks are missing**

|  |
| --- |
| **Risks** |
| False Authentication can be possible |
| Modification of data and injection of virus into systems. |
| The weak access points in the network will be known and can be used later to enter into the systems |
| Authentication of a fake individual can be possible |
| No guarantee that the sender is sending the information |
| False authorization to assets within the available staff is also harmful. |
| Getting external access into systems |
| Improper organization of data packets |
| Improper routing of data packets |
| Access of unwanted cookies into the system |
| Possible DOS attack |
| Violation of unused ports and protocols |
| Trust in business with clients will be lost |
| Password cracking becomes easy by brute force |

**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.**

* To prevent unauthorized access, two-factor authentication must be introduced which will help solve the problem to some extent.
* Proper storage must be given to the information by using the cloud services, hard disks, multiple computers to solve the problem of data loss.
* Proper safety must be followed during power-off time and data transfer time.
* Proper anti-virus must be installed in company computers to protect systems from unauthorized access and data modification.
* Security controls and policies must be considered and implemented until a required level to control the complexity.
* Proper routing configuration should be set up to understand a clear way of incoming and outgoing data packets.
* Firewall should be implemented with the requirements of the institution by keeping in mind ports and protocols.
* DMZ must be implemented to keep less important services to protect the important assets.
* VPN service must be enabled to provide safe networking with people at long distances.
* Proper port scanning must be enabled to monitor the traffic of data flow.
* Out of band and in-band management should be set up to keep the working of applications in place.
* SNMP must be implemented well for an organized working environment in the company.
* Cryptographic methods must be used to protect every form of data, code, and files.
* Company must make sure that all the business activities should not get stopped and work as per the regular schedule.
* Proper response should be given to government regarding the attack so that the company can get some help.
* Operations from the compromised systems must be stopped and replaced with new or backup systems to decrease the loss of the attack.
* The vulnerabilities regarding networks must be scanned after an attack and actions must be taken to implement hardware or software assistance.
* Defense – in – depth mechanism must provide layered security in case of a data breach.
* It must be ensured that a threat agent must not exploit other assets even though the network is compromised.
* Software code and applications must be verified whether they are modified, and they must be immediately restored to the previous version.
* The source of the problem must be identified whether it occurred from the network, OS or Software, and that vulnerability must be resolved.
* Updating software, cryptographic methods, and checking audit logs must be done from time to time.

**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:**

* Password-based management could be a serious problem if the passwords are small or easy to catch. So, there should be some rules for a password to set up to make a strong and qualified password. 2-factor authentication is required to increase security. Modern Artificial Intelligence like fingerprint scanners, facial recognition can also add added security.
* Using Relays in WAN server is having more residual risk from the above case. Security officials should be present to monitor data at such relay points, conducting security scans to protect data.
* By adding extra hardening controls like backing up the information in cloud or hard disks, password login, 2-factor authentication, we can protect such sensitive information.
* applying hardening controls like maintaining virus protection software, doing scans from time to time, password protection, information backup will help to protect LAN Server.
* Adopting modern cryptographic methodologies helps to add more security.
* Using devices like NIDS, Firewalls, Routers helps to observe the network traffic.

**For Kshemin Innovations PVT LTD:**

* To prevent unauthorized access, two-factor authentication must be introduced which will help solve the problem to some extent.
* Proper storage must be given to the information by using the cloud services, hard disks, multiple computers to solve the problem of data loss.
* Proper safety must be followed during power-off time and data transfer time.
* Proper anti-virus must be installed in company computers to protect systems from unauthorized access and data modification.
* Security controls and policies must be considered and implemented until a required level to control the complexity.
* Proper routing configuration should be set up to understand a clear way of incoming and outgoing data packets.
* Firewall should be implemented with the requirements of the institution by keeping in mind ports and protocols.
* DMZ must be implemented to keep less important services to protect the important assets.
* VPN service must be enabled to provide safe networking with people at long distances.
* Proper port scanning must be enabled to monitor the traffic of data flow.
* Out of band and in-band management should be set up to keep the working of applications in place.
* SNMP must be implemented well for an organized working environment in the company.
* Cryptographic methods must be used to protect every form of data, code, and files.
* Warning messages must be sent or printed if there is any slight modification of the existing data.
* Proper authentication techniques must be used for giving access to the database.
* Role-based authorization must be provided, and auditing of the files must be done.
* Network and Operating system must be checked from time to time, and it should be verified that there is no single access point for the outsiders.
* Role-based authorization must be provided, and auditing of the files must be done.
* IEEE standards and protocols must be followed strictly to ensure good security.
* Connectivity with Bluetooth and Wi-Fi must be verified as there can be open malicious networks.
* Company must make sure that all the business activities should not get stopped and work as per the regular schedule.
* Problem should be identified and should be analyzed by technological – management – operational teams.
* Proper response should be given to government regarding the attack so that the company can get some help.
* Operations from the compromised systems must be stopped and replaced with new or backup systems to decrease the loss of the attack.
* The vulnerabilities regarding networks must be scanned after an attack and actions must be taken to implement hardware or software assistance.
* Defense – in – depth mechanism must provide layered security in case of a data breach.
* It must be ensured that a threat agent must not exploit other assets even though the network is compromised.
* Important data must be stored in alternative hard drives and cloud services to protect in time of an attack.
* Software code and applications must be verified whether they are modified, and they must be immediately restored to the previous version.
* The source of the problem must be identified whether it occurred from the network, OS or Software, and that particular vulnerability must be resolved.
* Updating software, cryptographic methods, and checking audit logs must be done from time to time.

**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: $274750

Residual Risk with new controls: $32948

Proposed Security Risk Budget Cost: $230000

**Residual Risk Reduction**:

Residual Risk with current controls – Residual Risk with new controls

= $274750 - $32948 = $241802

This amount is more than proposed budget

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

Proposed security risk budget / expected security risk benefit

= $230000 / $241802 = 0.95

**For Kshemin Innovations PVT LTD:**

Residual Risk with current controls: $222800

Residual Risk with new controls: $45678

Proposed Security Risk Budget Cost: $160000

**Residual Risk Reduction**:

Residual Risk with current controls – Residual Risk with new controls

= $222800 - $45678 = $177122

This amount is more than proposed budget

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

Proposed security risk budget / expected security risk benefit

= $160000 / $177122 = 0.90

**Comparing the proposed security controls, methods, and policies budget for HGA with the proposed security controls, methods, and policies for Kshemin Innovations PVT LTD:**

|  |  |  |
| --- | --- | --- |
| **Points of consideration** | **HGA** | **Kshemin Innovations PVT LTD** |
| Industry | Financial - Government | Private – Data Analytics Modelling – Automobile based |
| Mission | Deals with release of funds to different government agencies | Gathers data from automobiles, process them to create data model and supplies output from a device manufactured by the company. |
| Geographic Presence | United States of America | Visakhapatnam, India |
| Number of Employees | 1000 | 125 |
| Network Topology | Appendix 3 | Appendix 4 |
| Critical Assets $ | $274750 | $222800 |
| Threat Environment | Nation State, Competitors, Hacker Organizations | Hackers, Commercial Groups, Disaffected Employee |
| Threat Agents | Terrorists, Criminals, Insiders | Insiders, Hackers, Terrorists |
| Residual Security Risks in $ | $32948 | $45678 |
| Budget for Risk Prevention and response controls, methods, policies | $230000 | $160000 |
| $ Security budget / $ Security Risk Improvement | 0.95 | 0.90 |
| $ Security budget / $ Critical Assets | 0.83 | 0.71 |
| $ Security budget / $ Employees | 230 | 1280 |

**Attack Tree for Hypothetical Government Agency (HGA):**

**Diagram

Description automatically generated**

**Attack Tree for Kshemin Innovations PVT LTD:**

**Diagram

Description automatically generated**

**Vulnerabilities and Exploitation Probabilities:**

**For HGA:**

|  |  |
| --- | --- |
| Vulnerability | Exploitation Probability |
| Improper storage of time and attendance information | 40 |
| Usage of relay points by WAN service provider | 35 |
| Including other accessible files in the email utility | 30 |
| Not running a virus scanner | 25 |
| Improper backup of information in storage devices | 35 |
| Unauthorized Access | 40 |
| Improper data modification applications in the server | 25 |
| Password-based management for a mainframe | 15 |

**For Kshemin Innovations PVT LTD:**

|  |  |
| --- | --- |
| Vulnerability | Exploitation Probability |
| Unauthorized Access | 35 |
| Firewall Setting | 30 |
| Adding malware patch to the software | 40 |
| Exposing key information | 15 |
| Improper Storage and Backup | 35 |
| Access to Confidential Information | 20 |
| Easy availability of an access point | 30 |
| Insider Access | 20 |

**Cybersecurity Workforce Recommendation:**

**For HGA:**

* Proper Training must be given regarding how to manage the risk and Incident Response.
* Employees must have knowledge regarding all aspects of the company to deal with any possible risk.
* Proper access and authorization controls must be implemented for the employees within the company.
* Sometimes, it requires individuals to make critical decisions on framing risk management plans. Such decisions must be planned to take the opinion of the group of individuals rather than a single person, to avoid biased opinions.
* Providing Authorization for various tasks based on the role is also important. Not every function must be accessible to every employee. Doing that will protect systems when an attack is done through a single user.

**For Kshemin Innovations PVT LTD:**

Based on the information that I have gathered for the company that I have contacted, it is mainly a startup company, and hence it requires a greater deal of management of the workforce with the growth of the company in the market. Presently, it is maintaining basic prevention and response strategies and minimum cybersecurity professionals to deal with the possible risks. But differentiation of employees based on skill and knowledge is important. Providing Authorization for various tasks based on the role is also important. Not every function must be accessible to every employee. Doing that will protect systems when an attack is done through a single user. A detailed management framework must be designed to always keep an eye on every individual because there can always be a malicious insider. Also, there must always be an individual who must have knowledge and skill to deal with every aspect of the organization like networks, software, business, and others because a potential risk can be interdisciplinary that can affect multiple zones. Training must be given for the employees to understand the work environment, vulnerabilities, and threats. Proper insights must be given regarding the procedure on how to report to the public federal agencies after an attack. Sometimes, it requires individuals to make critical decisions on framing risk management plans. Such decisions must be planned to take the opinion of the group of individuals rather than a single person, to avoid biased opinions.

**PART D: Appendix**

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

Diagram

Description automatically generated

This agency contains different blocks like multiple Local Area Networks (LAN), databases, mainframe computers, and others. These blocks are connected through a Wide Area Network (WAN). A local area network consists of a LAN server, console, router, modem pool, and other blocks. All these are considered as assets and are useful for specific purposes.

**Appendix 4: Detailed Network Topology (defense-in-depth) for Kshemin Innovations PVT LTD**

**Diagram

Description automatically generated**

The network infrastructure of Kshemin Innovations PVT LTD consists of servers, databases, cloud services, firewall, router, DMZ, and VPN. The information from the source computer is sent through the firewall and is routed to the destination address by the router. The data packets enter the destination firewall through the internet and get switched to various systems at the destination. The packets coming from the destination pass through the firewall as per the type of firewall and they enter DMZ, or the main system based on the type of input. VPN is used to provide access to a private network through the public network for a distant office.

**References**:

* Din, Antonia. “What Is Biometric Authentication? Definition, How It Works, Pros and Cons.” Heimdal Security Blog. Heimdal Security, October 13, 2021. https://heimdalsecurity.com/blog/biometric-authentication/#:~:text=%20Biometric%20Authentication%20Methods%20%201%20Fingerprint%20Scanners.,or%20both%20irises%20of%20a%20person.%20More%20.
* *What is defense in depth?* Forcepoint. (2021, May 6). Retrieved from https://www.forcepoint.com/cyber-edu/defense-depth
* *Firewall as a service*. Perimeter 81. (2022, April 17). Retrieved from https://www.perimeter81.com/firewall-as-a-service
* https://www.cac.mil/
* https://www.luc.edu/its/aboutits/itspoliciesguidelines/router\_and\_switch\_security\_standard.shtml#:~:text=Baseline%3A%201%20No%20local%20user%20accounts%20are%20configured,4%20Use%20SNMPv3%20and%20AES.%20More%20items...%20
* https://www.javatpoint.com/simple-network-management-protocol
* https://www.paloaltonetworks.com/cyberpedia/what-is-an-intrusion-detection-system-ids#:~:text=What%20is%20an%20Intrusion%20Detection%20System%3F%20%20,%201.%20Signature%20detection%3A%20-%20Exploit-facing%20...%20
* Namuag, P. *Database encryption: Why and where you need to have data encryption*. Severalnines. (2021, March 17). Retrieved from https://severalnines.com/database-blog/database-encryption-why-and-where-you-need-have-data-encryption#:~:text=Database%20encryption%20is%20a%20process%20to%20convert%20data,businesses%20dealing%20with%20financial%2C%20health%20care%2C%20or%20e-commerce.
* *Database administrator: Learn the working of data administrators*. EDUCBA. (2021, October 12). Retrieved from https://www.educba.com/database-administrator/
* *What is database security: Threats & best practices: Imperva*. Learning Center. (2021, November 8). Retrieved from https://www.imperva.com/learn/data-security/database-security/
* https://www.isaca.org/resources/isaca-journal/past-issues/2012/database-backup-and-recovery-best-practices
* Lutkevich, B., & Posey, B. *What is a race condition?* SearchStorage. (2021, June 16). Retrieved from https://www.techtarget.com/searchstorage/definition/race-condition
* *Software configuration management: Complete guide to SCM*. EDUCBA. (2021, March 1). Retrieved from https://www.educba.com/software-configuration-management/?msclkid=5c0fedbfb78511ec997712fff6dc3e50
* https://www.intruder.io/?utm\_source=bing&utm\_medium=cpc&utm\_campaign=USA|Search|Vulnerability|EX&utm\_term=website%20vulnerability%20scanner&msclkid=1b3503a098bf1ccf847361f035d60633
* Gopikrishnan, K. *The bluetooth standard - A simple guide to the protocol for beginners*. Technobyte. (2020, October 20). Retrieved from https://technobyte.org/bluetooth-standard-beginners-explained-guide/?msclkid=1a084265bd0311ecbb9ab5b1a5279fb6
* *Wi-Fi Standards explained*. GeeksforGeeks. (2021, March 17). Retrieved from https://www.geeksforgeeks.org/wi-fi-standards-explained/?msclkid=2fc4622bbd0311eca773e749622f754f