**HGA Risk Assessment Plan**

**CY5200 Security Risk Management**

**Module 4 Assignment**

**By Kalp Shah**

**Instructor: Prof Papageorge A. Themis**

**Table of Contents**

[**Executive Summary** 3](#_Toc157982848)

[**List of Assets** 9](#_Toc157982849)

[**List of Vulnerabilities** 11](#_Toc157982850)

[**List of Threats** 12](#_Toc157982851)

[**Threat Vulnerability pairs** 13](#_Toc157982852)

[**Assets impacted by Threat/Vulnerability pairs** 15](#_Toc157982853)

[**MOT controls covered by current HGA controls** 16](#_Toc157982854)

[**MOT controls covered by new CISO** 19](#_Toc157982855)

[**Risk Prevention Strategies** 21](#_Toc157982856)

[**Risk Resilience Strategies** 24](#_Toc157982857)

[**Optimized Mixed Security Strategies** 29](#_Toc157982858)

[**Conclusion** 37](#_Toc157982859)

# **Executive Summary**

**Information System Name:** Hypothetical Government Agency

**Information System Categorization:**

|  |  |  |  |
| --- | --- | --- | --- |
| **Assets** | **Information Security Elements** | | |
| **Confidentiality** | **Integrity** | **Availability** |
| Financial Resources | High | High | High |
| Sensitive Documents | High | High | High |
| Personnel Information | High | High | High |
| Reports and Policies | High | High | High |
| Physical Entities and Hardware | High | High | High |
| Applications and Software | High | High | High |

**Organization Name:** Hypothetical Government Agency

**Organization Address:** 152 Newburry Street, Boston, MA – 02312

**Senior Management:**

**Nency Shah**

**Title:** Chief Executive Officer

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

**Phone:** +1 857 369 2102

**Ramya Doshi**

**Title:** Chief Financial Officer

**Email:** ram.dos@hga.gov

**Phone:** +1 893 664 1987

**John Snow**

**Title:** Chief Information Officer

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

**Phone:** +1 996 201 5576

**Patrick Lyod**

**Title:** Chief Information Security Officer

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

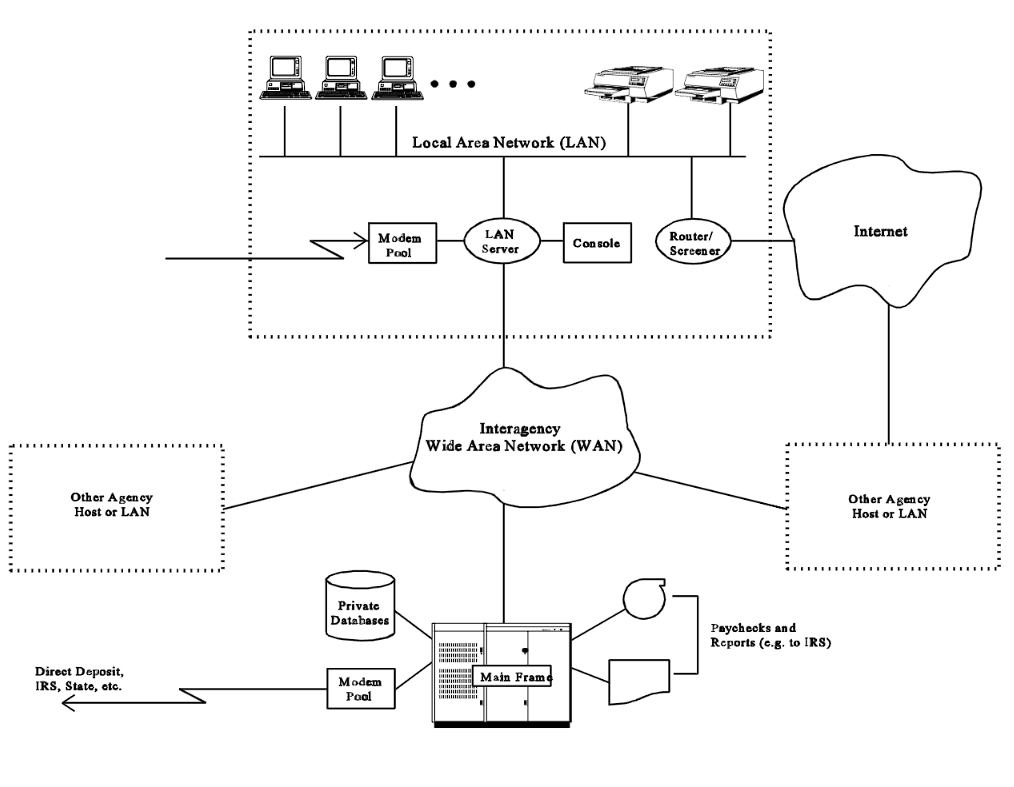
**Phone:** +1 455 363 0025

**Information system operational status:** Operational

**Information System Type:** Major Application

**System Description:** Ecosystem within the federal agencies supported by the mainframe and WAN to facilitate funds transfers and transactions to the employees associated with the federal agencies.

**System Environment:**

****

The above topology depicts HGA environment and the other federal connecting components. The assets of HGA are connected and can be communicated using LAN server internally. For external communication, with the main mainframe or other agency, WAN is used. Also, internet connection is provided via router. The employees travelling can also communicate via modem pool with a restricted access.

**Interconnection of System Information:**

**System Name:** Government Agency

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

**Type of Agreement:** Government Contract

**Date:** October 8, 2023

**FIPS 199 Category:** High

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

**Authorizing Official:** John Snow

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

* Federal Information Security Management Act (FISMA)
* ISO 27001
* ISO 22301
* NIST Cybersecurity Framework
* Sarbanes-Oxley Act
* US Privacy Act of 1974
* Gramm-Leach-Bliley Act (GLBA)

**Minimum Security Controls:**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Security Controls** | **Observations** | **Status** | **Control type** | **Responsible authority** |
| Policies(M1) | Rules and regulations to implement with compliant to different laws, frameworks and policies. | Partial | Common | CIO |
| Program Management(M2) | Strategical implementation of the policies to protect the assets. | Partial | Common | CIO |
| Risk Management(M3) | Calculation of risk with the reference of assets, threats, vulnerabilities, current controls, new controls and different strategies. | Complete | Common | CISO |
| Assurance(M4) | Ensures business continuity at the times of attacks. | Partial | Common | CISO |
| Preparing for Contingencies and Disasters(M5) | Reviewing, modifying, and formulating plans and policies in times of attack, contingencies, and natural disasters. | Partial | Common | CIO |
| Incident Handling and Reporting(M6) | Monitoring networks and connections. Detecting potential attacks or exploitation using tool type SIEM and report it. | Partial | Common | CISO |
| Awareness, Training and Education(M7) | Regular awareness and training on security practices and policies | Partial | Common | CISO |
| Physical and Environmental Security(M8) | With the digital security, securing databases, documents, and other artifacts valuable to the HGA | Partial | Common | CISO |
| Identification and Authentication(M9) | Implementing various methods like 2FA and biometrics for authorized access in a restrictive manner. | Partial | Common | CISO |
| Logical Access Control(M10) | Principle of least privilege to give very limited access and implementing restrictions for unauthorized users. | Complete | Common | CISO |
| Audit Trails(M11) | Investigating the logs and activity of assets to identify, detect and minimize the probability of anomalies and even it is done in the event of post-attack | Complete | Common | CISO |
| Cryptography(M12) | Encrypting data and communication channels to minimize effect of eavesdropping and data theft. | Partial | Common | CISO |

Information Security Plan Completion date: 12/15/2023

Information Security Plan Approval date: 02/04/2024

# **List of Assets**

The HGA contains:

40 PCS with each PC costs $1000.

5 Printers with each Printer costs $1000

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Asset** | **Description** | **$ Value** |
| A1 | Financial Resources | Includes paychecks, transfers, and balances | 10,000,000 |
| A2 | Personnel Information | Includes information about the employees like name, email addresses, paycheck details etc. | 50,000 |
| A3 | Documents | Includes draft regulations, contracts and procurement documents, draft regulations, reports, and memos. | 10,000 |
| A4 | PC | Hardware entity for personnels of HGA for their duties like submitting timesheets. | 40,000 |
| A5 | Employee Confidence | Crucial asset for HGA displaying trust for the agency. | 10,000 |
| A6 | Reputation | Intangible asset pertaining image and credibility of HGA. | 12,000 |
| A7 | Mainframe | Storage and retrieval medium of the databases from other agencies. | 30,000 |
| A8 | LAN Server | Central network component between PCs and other hardware entities and shared programs, storage etc. | 30,000 |
| A9 | Storage | Databases for storing general and sensitive information both regarding financials and personnels. | 5,000 |
| A10 | WAN | Connects different agencies LAN networks and mainframe for information sharing and smooth communications | 5,000 |
| A12 | Modem Pool | Service for employees who are travelling for checking emails and dial-ins. | 1,000 |
| A13 | Console | Interface for server administrators to perform sensitive and crucial tasks securely. | 3,000 |
| A14 | Printers | For printouts of documents via LAN by HGA employees. | 5,000 |
| A15 | Router | Provides an internet connection and protocol translation. | 1,000 |
| A16 | Programs and Tools | Interface for HGA personnels to perform their duties. | 4,500 |

# **List of Vulnerabilities**

|  |  |
| --- | --- |
|  | **Vulnerability** |
| V1 | Falsified Timesheets |
| V2 | Unauthorized Access |
| V3 | Bogus Time and Attendance Applications |
| V4 | Unauthorized Modification of the data |
| V5 | Payroll Errors |
| V6 | Lack of Contingency Planning |
| V7 | Virus/Malware spread |
| V8 | Corruption and Loss of Data |
| V9 | Network Related |
| V10 | Lack of physical security |
| V11 | Inadequate security of storage, database, and mainframe |
| V12 | Employee not compliant of PCs security |

# **List of Threats**

|  |  |
| --- | --- |
| **Number** | **Threat** |
| T1 | Payroll Frauds |
| T2 | Payroll Errors |
| T3 | Interruption of Operations |
| T4 | Disclosure and Brokerage of Information |
| T5 | Network related Threats |
| T6 | Virus and Malware |
| T7 | Unauthorized Access |
| T8 | Theft |
| T9 | Natural Disaster |

# **Threat Vulnerability pairs**

|  |  |
| --- | --- |
| **Number** | **Threat** |
| T1 | Payroll Frauds |
| T3 | Interruption of Operations |
| T4 | Disclosure and Brokerage of Information |
| T9 | Natural Disaster |

|  |  |
| --- | --- |
| **Number** | **Vulnerability** |
| V1 | Falsified Timesheets |
| V2 | Unauthorized Access |
| V8 | Corruption and Loss of Data |
| V11 | Inadequate security of storage, database, and mainframe |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | 95 | 90 | 90 | 85 |
| V2 on A2, A4, A8 | 90 | 90 | 95 | 85 |
| V8 on A1, A2, A4, A8 | 90 | 90 | 85 | 95 |
| V11 on A1, A2 | 90 | 95 | 95 | 80 |

**Explanation to the assigned values of selected threats**

**Payroll fraud** is very critical. It is one of the most common threats that leads to significant loss of the agencies. This financial fraud generally exploits lack of authentication and authorization measures along with irregular audit and security checks.

**Interruption of Operations** is very important for the HGA. The reputation is directly connected to this threat along with the employee confidence. Hindering operations can lead to significant delay in paying the personnels of all federal agencies which is a crucial and most important sector of any nation.

**Disclosure and Brokerage of Information** can cause great damage. Such threat affects the sensitive information of the financial assets and personnels that not only breach trust and reputation but can also be misused for malicious purposes.

**Natural Disasters** could be small or could be catastrophic. In any case, the destruction of property in terms of information or hardware results in a serious loss to HGA and all other agencies linked to it.

# **Assets impacted by Threat/Vulnerability pairs**

|  |  |
| --- | --- |
| **Asset** | **Vulnerability** |
| A1 Financial Resources | V1 Falsified Timesheets  V8 Corruption and Loss of Data  V11 Inadequate security of storage, database, and mainframe |
| A2 Personnel Information | V1 Falsified Timesheets  V2 Unauthorized Access  V8 Corruption and Loss of Data  V11 Inadequate security of storage, database, and mainframe |
| A4 PC | V2 Unauthorized Access  V8 Corruption and Loss of Data |
| A8 LAN Server | V2 Unauthorized Access  V8 Corruption and Loss of Data |

# **MOT controls covered by current HGA controls**

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Category** | **Description** | **MOT Controls** |
| CSCP 1 | Security Manual | In compliance with federal and financial policies | 1 |
| CSCP 2 | General Use | Duties and privileges segregation of personnels | 2,3,5,6 |
| CSCP 3 | General | Security awareness training | 3,4,7 |
| CSCP 4 | General | Password selection and security policy | 1,3 |
| CSCP 5 | General | Access Control Mechanism | 4,6,9,10 |
| CSCP 6 | Payroll Frauds and Errors | Time and attendance application | 10,11 |
| CSCP 7 | Payroll Frauds and Errors | Sign and submit time sheet | 10,11 |
| CSCP 8 | Payroll Frauds and Errors | Data validation, verification, and authorization | 4,9,10,11 |
| CSCP 9 | Payroll Frauds and Errors | Access control and identification | 4,6,9,10 |
| CSCP 10 | Payroll Frauds and Errors | Containerization of the server | 5 |
| CSCP 11 | Payroll Frauds and Errors | Time sheet verification twice and sanity checks | 4 |
| CSCP 12 | Payroll Frauds and Errors | Segregation of personnel duties | 2 |
| CSCP 13 | Payroll Frauds and Errors | Digital signature for integrity | 4,12 |
| CSCP 14 | Payroll Frauds and Errors | Regular backup | 3,4,5 |
| CSCP 15 | Interruption of Operations | COG Contingency Planning and Testing | 3,4,6 |
| CSCP 16 | Interruption of Operations | Spare PCs, LAN server and cables, and drives in case of malfunctions | 3,5 |
| CSCP 17 | Interruption of Operations | Installation of licensed software and regular installation of patches | 1,2 |
| CSCP 18 | Interruption of Operations | Log Audit | 6,11 |
| CSCP 19 | Interruption of Operations | Division Contingency Planning | 3,4,6 |
| CSCP 20 | Disclosure or Brokerage of Information | Need to know policy | 1,3,9 |
| CSCP 21 | Disclosure or Brokerage of Information | Secure and guard physical and digital storage | 5,8 |
| CSCP 22 | Disclosure or Brokerage of Information | Policy on PC locks | 1,4,7,8,10 |
| CSCP 23 | Disclosure or Brokerage of Information | Group oriented access control | 10 |
| CSCP 24 | Disclosure or Brokerage of Information | Security awareness training | 3,7 |
| CSCP 25 | Network Threats | Filtered and restricted network activity | 4,12 |
| CSCP 26 | Network Threats | Packets monitoring | 11 |
| CSCP 27 | Network Threats | Restricted remote logins and dial-in access | 9,10 |
| CSCP 28 | Non-HGA Computer Systems | Policy for the HGA system components provided by external organization | 1,3,4 |

# **MOT controls covered by new CISO**

|  |  |  |  |
| --- | --- | --- | --- |
| **Number** | **Category** | **Description** | **MOT Controls** |
| NSP 1 | Payroll Frauds | Advanced authentication mechanisms(smart tokens for One Time Password) | 4,9,10 |
| NSP 2 | Payroll Frauds | Administrative Procedures | 1,2,7 |
| NSP 3 | Payroll Frauds | Monitoring | 6,11 |
| NSP 4 | Payroll Frauds | Implement cryptographic techniques – Digital Signature | 12 |
| NSP 5 | Payroll Errors | Greater and improved compliance based on incentive system | 2,4,7 |
| NSP 6 | Continuity of Operations | Regular internal training and awareness sessions | 1,7,8 |
| NSP 7 | Continuity of Operations | Contingency plan rehearsal | 2,3,5,8 |
| NSP 8 | Continuity of Operations | Virus Prevention procedures | 1,3,6,71,10 |
| NSP 9 | Continuity of Operations | Improved backup procedures | 2,4,5 |
| NSP 10 | Information Disclosure/Brokering | Enhanced security refresher courses | 1,2,7 |
| NSP 11 | Information Disclosure/Brokering | Changes in storage policy for sensitive information | 1,3,4 |
| NSP 12 | Information Disclosure/Brokering | Installing and reviewing activity logs | 1,11 |
| NSP 13 | Network Threats | Stronger Identity and Access Management controls for dial-in | 9,10 |
| NSP 14 | Network Threats | Restricting sensitive outbound traffic | 9,10 |
| NSP 15 | Network Threats | Encrypted modems | 12 |
| NSP 16 | Network Threats | Inbound and outbound traffic encryption via WAN | 12 |

# **Risk Prevention Strategies**

Implementing current controls, new CISO controls, missing MOT controls, 2FA, VPN, and DMZ reduces the likelihood of many threats. Along with, the vulnerability exploitation probabilities are also reduced. Here, 2FA provides us identification, authentication and access control. VPN provides network tunneling along with acting as proxy protecting the infrastructure from the direct exposure. DMZ acts a decoy being a layer about actual server and database which if attacked does not affects the actual server and database.

**Threat Vulnerability Pair**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | 30 | 35 | 35 | 40 |
| V2 on A2, A4, A8 | 30 | 35 | 35 | 40 |
| V8 on A1, A2, A4, A8 | 10 | 5 | 5 | 10 |
| V11 on A1, A2 | 40 | 35 | 30 | 35 |

**Residual Asset Security Risks**

Risk of asset A1: 1000000\*(30+35+35+40+10+5+5+10+40+35+30+35)/ 100 = 31000000

Risk of asset A2:

50000 \* (30+35+35+40+30+35+35+40+10+5+5+10+40+35+30+35)/100 = 225000

Risk of asset A4: 40000 \* (30+35+35+40+30+35+35+40+10+5+5+10)/100 = 124000

Risk of asset A8: 30000 \* (30+35+35+40+10+5+5+10)/100 = 51000

**Residual Vulnerability Security Risk**

Risk due to V1: [(10,000,000\*140) + (50000 \*140) + (40000\*140)] / 100 = 14126000

Risk due to V2: [(50000 \*140) + (40000\*140) + (30000 \*140)] / 100 = 168000

Risk due to V8: [(10,000,000\*30) + (50000 \*30) + (40000\*30) + (30000 \*30)] / 100 = 3036000

Risk due to V11: [(10,000,000\*140) + (50000 \*140)] / 100 = 14070000

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A1 | 31000000 | 1 |
| A2 | 225000 | 2 |
| A4 | 124000 | 3 |
| A8 | 51000 | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V1 | 14126000 | 1 |
| V11 | 14070000 | 2 |
| V8 | 3036000 | 3 |
| V2 | 168000 | 4 |

**Prevention Strategy Step P2:**

**Threat Vulnerability Pair**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | 5 | 5 | 3 | 10 |
| V2 on A2, A4, A8 | 30 | 35 | 35 | 40 |
| V8 on A1, A2, A4, A8 | 10 | 5 | 5 | 10 |
| V11 on A1, A2 | 40 | 35 | 30 | 35 |

**Residual Asset Security Risks**

Risk of asset A1: 1000000\*(5+5+3+10+10+5+5+10+40+35+30+35)/ 100 = 19300000

Risk of asset A2:

50000 \* (5+5+3+10+30+35+35+40+10+5+5+10+40+35+30+35)/100 = 166500

Risk of asset A4: 40000 \* (5+5+3+10+30+35+35+40+10+5+5+10)/100 = 124000

Risk of asset A8: 30000 \* (30+35+35+40+10+5+5+10)/100 = 51000

**Residual Vulnerability Security Risk**

Risk due to V1: [(10,000,000\*23) + (50000 \*23) + (40000\*23)] / 100 = 2320700

Risk due to V2: [(50000 \*140) + (40000\*140) + (30000 \*140)] / 100 = 168000

Risk due to V8: [(10,000,000\*30) + (50000 \*30) + (40000\*30) + (30000 \*30)] / 100 = 3036000

Risk due to V11: [(10,000,000\*140) + (50000 \*140)] / 100 = 14070000

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A1 | 19300000 | 1 |
| A2 | 166500 | 2 |
| A4 | 124000 | 3 |
| A8 | 51000 | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V11 | 14070000 | 1 |
| V8 | 3036000 | 2 |
| V1 | 2320700 | 3 |
| V2 | 168000 | 4 |

# **Risk Resilience Strategies**

Implementing current controls, new CISO controls, missing MOT controls, Redudant server, and Mirror site. It reduces the likelihood of many threats. Along with, the vulnerability exploitation probabilities are also reduced. Here both redundant server and mirror site acts as in business continuity components where in case of an attack, if any server or sites goes down the backup ones could be made live in order to make the operations flowing.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | T1 | T3 | T4 | T9 |
| V1 on A1, A2, A4 | 5 | 10 | 10 | 5 |
| V2 on A2, A4, A8 | 5 | 5 | 3 | 10 |
| V8 on A1, A2, A4, A8 | 10 | 5 | 5 | 10 |
| V11 on A1, A2 | 3 | 5 | 10 | 5 |

**Updated Risk Impacts**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T3xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | 60% | 0 | 0 | 0 | 0 | 0 | 50% | 0 | 0 | 0 | 0 | 50% | 0 | 0 | 40% | 0 |
| A2 | 60% | 0 | 0 | 0 | 0 | 50% | 60% | 0 | 0 | 70% | 0 | 40% | 0 | 0 | 50% | 0 |
| A4 | 70% | 0 | 0 | 0 | 0 | 60% | 50% | 0 | 0 | 60% | 0 | 0 | 0 | 0 | 50% | 0 |
| A8 | 0 | 0 | 0 | 0 | 0 | 70% | 50% | 0 | 0 | 50% | 0 | 0 | 0 | 0 | 60% | 0 |

**Residual Asset Security Risk**

Risk of Asset A1 :

1000000 \* (5\*60 + 5\*50 + 10\*50 + 10\*40 )/100 = 1450000

Risk of Asset A2 :

50000 \* (5\*60 + 5\*50 + 5\*60 + 3\*70 + 10\*40 + 10\*50 )/100 = 9800

Risk of Asset A4 :

40000 \* (5\*70 + 5\*60 + 5\*50 + 3\*50 + 10\*50)/100 = 6320

Risk of Asset A8 :

30000 \* (5\*60 + 5\*50 + 3\*70 + 10\*40)/100 = 4050

**Residual Asset Security Risk**

Risk due to V1: 1000000 \*(5\*60 ) + 50000 \*(5\*60 ) + 30000 \*(5\*70 ) = 302900

Risk due to V2: 95\*(5\*50+3\*70) + 40000\*(5\*60+3\*60) + 30000\*(5\*70+3\*50) = 5720

Risk due to V8: 1000000 \* (5\*50 + 10\*40) + 50000\*(5\*60+10\*50) + 40000\*(5\*50+10\*50) + 30000\*(3\*50+10\*60) = 659550

Risk due to V11: 1000000\*(10\*50) + 50000\*(10\*40) = 502000

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A1 | 1450000 | 1 |
| A2 | 9800 | 2 |
| A4 | 6320 | 3 |
| A8 | 4050 | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V8 | 659550 | 1 |
| V11 | 502000 | 2 |
| V1 | 302900 | 3 |
| V2 | 5720 | 4 |

**Response (Resilience) Strategy Step RE2**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **Threat x Vulnerability** | | | | | | | | | | | | | | | |
|  | T1xV1 | T1xV2 | T1xV8 | T1xV11 | T3xV1 | T3xV2 | T3xV8 | T3xV11 | T3xV1 | T4xV2 | T4xV8 | T4xV11 | T9xV1 | T9xV2 | T9xV8 | T9xV11 |
| A1 | 20% | 0 | 0 | 0 | 0 | 0 | 10% | 0 | 0 | 0 | 0 | 10% | 0 | 0 | 10% | 0 |
| A2 | 60% | 0 | 0 | 0 | 0 | 50% | 60% | 0 | 0 | 70% | 0 | 40% | 0 | 0 | 50% | 0 |
| A4 | 70% | 0 | 0 | 0 | 0 | 60% | 50% | 0 | 0 | 60% | 0 | 0 | 0 | 0 | 50% | 0 |
| A8 | 0 | 0 | 0 | 0 | 0 | 70% | 50% | 0 | 0 | 50% | 0 | 0 | 0 | 0 | 60% | 0 |

**Residual Asset Security Risk**

Risk of Asset A1 :

1000000 \* (5\*20 + 5\*10 + 10\*10 + 10\*10 )/100 = 350000

Risk of Asset A2 :

50000 \* (5\*60 + 5\*50 + 5\*60 + 3\*70 + 10\*40 + 10\*50 )/100 = 9800

Risk of Asset A4 :

40000 \* (5\*70 + 5\*60 + 5\*50 + 3\*50 + 10\*50)/100 = 6320

Risk of Asset A8 :

30000 \* (5\*60 + 5\*50 + 3\*70 + 10\*40)/100 = 4050

**Residual Asset Security Risk**

Risk due to V1: 1000000 \*(5\*20 ) + 50000 \*(5\*60 ) + 30000 \*(5\*70 ) = 302900

Risk due to V2: 95\*(5\*50+3\*70) + 40000\*(5\*60+3\*60) + 30000\*(5\*70+3\*50) = 5720

Risk due to V8: 1000000 \* (5\*10 + 10\*40) + 50000\*(5\*60+10\*50) + 40000\*(5\*50+10\*50) + 30000\*(3\*50+10\*60) = 659550

Risk due to V11: 1000000\*(10\*10) + 50000\*(10\*40) = 502000

**Ranking of residual asset security risks**

|  |  |  |
| --- | --- | --- |
| **Asset** | **Residual Security Risk** | **Ranking** |
| A1 | 750000 | 1 |
| A2 | 9800 | 2 |
| A4 | 6320 | 3 |
| A8 | 4050 | 4 |

**Ranking of residual vulnerability security risks**

|  |  |  |
| --- | --- | --- |
| **Vulnerability** | **Residual Security Risk** | **Ranking** |
| V8 | 159550 | 1 |
| V1 | 102900 | 2 |
| V11 | 102000 | 3 |
| V2 | 5720 | 4 |

# **Optimized Mixed Security Strategies**

**Mixed Strategy Step 1: Start with TV and RI from Scenario 3 and apply 2-Factor Authentication. The results should be the same as above.**

**TV Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T1 | T2 | T3 | T4 | Total |
| V1 on A1, A2, A4 | 20 | 25 | 25 | 35 | 105 |
| V2 on A2, A4, A8 | 25 | 20 | 20 | 30 | 95 |
| V8 on A1, A2, A4, A8 | 30 | 25 | 20 | 30 | 105 |
| V11 on A1, A2 | 30 | 25 | 25 | 25 | 105 |
| Total |  |  |  |  | 410 |

**RI Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **T1XV1** | **T1XV2** | **T1XV8** | **T1XV11** | **T3XV1** | **T3XV2** | **T3XV8** | **T3XV11** | **T4XV1** | **T4XV2** | **T4V8** | **T4XV11** | **T9XV1** | **T9XV2** | **T9XV8** | **T9XV11** |
| **A1** | **50%** | **0** | **0** | **0** | **0** | **0** | **70%** | **0** | **0** | **0** | **0** | **70%** | **0** | **0** | **60%** | **0** |
| **A2** | **40%** | **0** | **0** | **0** | **0** | **35%** | **60%** | **0** | **0** | **60%** | **0** | **70%** | **0** | **0** | **50%** | **0** |
| **A4** | **40%** | **0** | **0** | **0** | **0** | **50%** | **60%** | **0** | **0** | **40%** | **0** | **0** | **0** | **0** | **50%** | **0** |
| **A8** | **0** | **0** | **0** | **0** | **0** | **60%** | **50%** | **0** | **0** | **50%** | **0** | **0** | **0** | **0** | **60%** | **0** |

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Value | Total Threat | Residual Risk |
| A1 | 10,000,000 | 410 | 6300000.00 |
| A2 | 50,000 | 410 | 37250.00 |
| A4 | 40,000 | 410 | 22400.00 |
| A8 | 30,000 | 410 | 15750.00 |

|  |  |
| --- | --- |
| Vulnerability | Redisual Risk |
| V1 | 1007200.00 |
| V2 | 23300.00 |
| V8 | 3586150.00 |
| V11 | 1758750.00 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets** | | **Residual Risk** | | | |
| **A1** | | 6300000 | | | |
| **A2** | | 37250 | | | |
| **A4** | | 22400 | | | |
| **A8** | | 15750 | | | |
| **Investment** | 300000 | **Total Risk** | 6375400 | **ROI** | 12052.2 |

**Mixed Strategy Step 2: Start with TV and RI from Scenario 3 and apply VPN. Estimate updated Residual Critical Asset Risk rankings, Total Asset Risk, and Vulnerability Risk rankings.**

**TV Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T1 | T2 | T3 | T4 | Total |
| V1 on A1, A2, A4 | 30 | 35 | 35 | 40 | 140 |
| **V2 on A2, A4, A8** | **20** | **15** | **10** | **20** | **65** |
| V8 on A1, A2, A4, A8 | 40 | 35 | 30 | 35 | 140 |
| **V11 on A1, A2** | **25** | **20** | **15** | **20** | **80** |
| Total |  |  |  |  | 425 |

**RI Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **T1XV1** | **T1XV2** | **T1XV8** | **T1XV11** | **T2XV1** | **T2XV2** | **T2XV8** | **T2XV11** | **T3XV1** | **T3XV2** | **T3V8** | **T3XV11** | **T4XV1** | **T4XV2** | **T4XV8** | **T4XV11** |
| **A1** | **50** | **0** | **0** | **0** | **0** | **0** | **70** | **0** | **0** | **0** | **0** | **30** | **0** | **0** | **60** | **0** |
| **A2** | **40** | **0** | **0** | **0** | **0** | **25** | **60** | **0** | **0** | **30** | **0** | **35** | **0** | **0** | **50** | **0** |
| **A4** | **40** | **0** | **0** | **0** | **0** | **30** | **60** | **0** | **0** | **20** | **0** | **0** | **0** | **0** | **50** | **0** |
| **A8** | **0** | **0** | **0** | **0** | **0** | **40** | **50** | **0** | **0** | **25** | **0** | **0** | **0** | **0** | **60** | **0** |

|  |  |
| --- | --- |
| Vulnerability | Redisual Risk |
| V1 | 1510800 |
| V2 | 8525 |
| V8 | 4596200 |
| V11 | 452625 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets** | | **Residual Risk** | | | |
| **A1** | | 6500000 | | | |
| **A2** | | 31250 | | | |
| **A4** | | 22800 | | | |
| **A8** | | 14100 | | | |
| **Investment** | 400000 | **Total Risk** | 6568150 | **ROI** | 8990.9625 |

**Mixed Strategy Step 3: Start with TV and RI from Scenario 3 and apply DMZ. Estimate updated Residual Critical Asset Risk rankings, Total Asset Risk, and Vulnerability Risk rankings.**

**TV Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T1 | T2 | T3 | T4 | Total |
| V1 on A1, A2, A4 | 30 | 35 | 35 | 40 | 140 |
| V2 on A2, A4, A8 | 30 | 35 | 35 | 40 | 140 |
| V8 on A1, A2, A4, A8 | 40 | 35 | 30 | 35 | 140 |
| V11 on A1, A2 | **20** | **15** | **10** | **15** | **60** |
| Total |  |  |  |  | 480 |

**RI Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **T1XV1** | **T1XV2** | **T1XV8** | **T1XV11** | **T2XV1** | **T2XV2** | **T2XV8** | **T2XV11** | **T3XV1** | **T3XV2** | **T3V8** | **T3XV11** | **T4XV1** | **T4XV2** | **T4XV8** | **T4XV11** |
| **A1** | **50** | **0** | **0** | **0** | **0** | **0** | **70** | **0** | **0** | **0** | **0** | **25** | **0** | **0** | **60** | **0** |
| **A2** | **40** | **0** | **0** | **0** | **0** | **35** | **60** | **0** | **0** | **60** | **0** | **29** | **0** | **0** | **50** | **0** |
| **A4** | **40** | **0** | **0** | **0** | **0** | **50** | **60** | **0** | **0** | **40** | **0** | **0** | **0** | **0** | **50** | **0** |
| **A8** | **0** | **0** | **0** | **0** | **0** | **60** | **50** | **0** | **0** | **50** | **0** | **0** | **0** | **0** | **60** | **0** |

|  |  |  |  |
| --- | --- | --- | --- |
| Asset | Value | Total Threat | Residual Risk |
| A1 | 10,000,000 | 480 | 6300000 |
| A2 | 50,000 | 480 | 43325 |
| A4 | 40,000 | 480 | 32800 |
| A8 | 30,000 | 480 | 23100 |
| Vulnerability | Redisual Risk |
| V1 | 1510800 |
| V2 | 40775 |
| V8 | 4596200 |
| V11 | 251450 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets** | | **Residual Risk** | | | |
| **A1** | | 6300000 | | | |
| **A2** | | 43325 | | | |
| **A4** | | 32800 | | | |
| **A8** | | 23100 | | | |
| **Investment** | 400000 | **Total Risk** | 6399225 | **ROI** | 9033.19375 |

**Mixed Strategy Step 4: Start with TV and RI from Scenario 3 and apply Mirror Site. Estimate updated Residual Critical Asset Risk rankings, Total Asset Risk, and Vulnerability Risk rankings.**

**TV Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T1 | T2 | T3 | T4 | Total |
| V1 on A1, A2, A4 | 30 | 35 | 35 | 40 | 140 |
| V2 on A2, A4, A8 | 30 | 35 | 35 | 40 | 140 |
| V8 on A1, A2, A4, A8 | **20** | **20** | **20** | **10** | 70 |
| V11 on A1, A2 | **20** | **15** | **10** | **15** | **60** |
| Total |  |  |  |  | 410 |

**RI Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **T1XV1** | **T1XV2** | **T1XV8** | **T1XV11** | **T2XV1** | **T2XV2** | **T2XV8** | **T2XV11** | **T3XV1** | **T3XV2** | **T3V8** | **T3XV11** | **T4XV1** | **T4XV2** | **T4XV8** | **T4XV11** |
| **A1** | **50** | **0** | **0** | **0** | **0** | **0** | **35** | **0** | **0** | **0** | **0** | **15** | **0** | **0** | **25** | **0** |
| **A2** | **40** | **0** | **0** | **0** | **0** | **35** | **30** | **0** | **0** | **60** | **0** | **10** | **0** | **0** | **20** | **0** |
| **A4** | **40** | **0** | **0** | **0** | **0** | **50** | **25** | **0** | **0** | **40** | **0** | **0** | **0** | **0** | **25** | **0** |
| **A8** | **0** | **0** | **0** | **0** | **0** | **60** | **20** | **0** | **0** | **50** | **0** | **0** | **0** | **0** | **15** | **0** |

|  |  |
| --- | --- |
| Vulnerability | Redisual Risk |
| V1 | 1510800 |
| V2 | 407750 |
| V8 | 958650 |
| V11 | 150500 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets** | | **Residual Risk** | | | |
| **A1** | | 2600000 | | | |
| **A2** | | 27125 | | | |
| **A4** | | 20400 | | | |
| **A8** | | 13200 | | | |
| **Investment** | 600000 | **Total Risk** | 2660725 | **ROI** | 6645.2125 |

**Mixed Strategy Step 5: Start with TV and RI from Scenario 3 and apply Mirror Site. Estimate updated Residual Critical Asset Risk rankings, Total Asset Risk, and Vulnerability Risk rankings.**

**TV Matrix**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
|  | T1 | T2 | T3 | T4 | Total |
| V1 on A1, A2, A4 | **20** | **15** | **15** | **10** | **60** |
| V2 on A2, A4, A8 | 30 | 35 | 35 | 40 | 140 |
| V8 on A1, A2, A4, A8 | 40 | 35 | 30 | 35 | 140 |
| V11 on A1, A2 | 40 | 35 | 30 | 35 | 140 |
| Total |  |  |  |  | 480 |

**RI Matrix**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| **Assets** | **T1XV1** | **T1XV2** | **T1XV8** | **T1XV11** | **T2XV1** | **T2XV2** | **T2XV8** | **T2XV11** | **T3XV1** | **T3XV2** | **T3V8** | **T3XV11** | **T4XV1** | **T4XV2** | **T4XV8** | **T4XV11** |
| **A1** | **20** | **0** | **0** | **0** | **0** | **0** | **70** | **0** | **0** | **0** | **0** | **70** | **0** | **0** | **60** | **0** |
| **A2** | **15** | **0** | **0** | **0** | **0** | **35** | **60** | **0** | **0** | **60** | **0** | **70** | **0** | **0** | **50** | **0** |
| **A4** | **10** | **0** | **0** | **0** | **0** | **50** | **60** | **0** | **0** | **40** | **0** | **0** | **0** | **0** | **50** | **0** |
| **A8** | **0** | **0** | **0** | **0** | **0** | **60** | **50** | **0** | **0** | **50** | **0** | **0** | **0** | **0** | **60** | **0** |

|  |  |
| --- | --- |
| Vulnerability | Redisual Risk |
| V1 | 402300 |
| V2 | 40775 |
| V8 | 4596200 |
| V11 | 2110500 |

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Assets** | | **Residual Risk** | | | |
| **A1** | | 7050000 | | | |
| **A2** | | 47875 | | | |
| **A4** | | 28800 | | | |
| **A8** | | 23100 | | | |
| **Investment** | 400000 | **Total Risk** | 7149775 | **ROI** | 8845.55625 |

**Mixed strategy budget to minimize Asset Risk:**

|  |  |
| --- | --- |
| **Implemented Controls** | **Cost** |
| 2FA | 300000 |
| VPN | 400000 |
| DMZ | 400000 |
| Redundant Server | 600000 |
| Mirror Site | 400000 |

**Total Budget : 2100000**

**Mixed strategy budget to maximize ROI:**

|  |  |  |
| --- | --- | --- |
| **Rank** | **Implemented Controls** | **ROI** |
| 1 | 2FA | 12052.2 |
| 2 | DMZ | 9033.19375 |
| 3 | VPN | 8990.9625 |
| 4 | Mirror Site | 8845.55625 |
| 5 | Redudant Server | 6645.2125 |

# **Conclusion**

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

HGA teams almost addressed all security risks. The current controls lacked many MOT controls that could have implemented. However, after implementing new CISO recommendations controls, it covered wide range of security risks. To add one, the physical and environmental security could have been also stressed on. There are very partial implementation of the physical sescurity. This is also crucial miss out as sensitive documents, various hardware, etc. are vulnerable to threats like theft and disclosure of information. aking a scenario, it lacked authentication measures, which would have reduced some of the biggest threats like failure to maintain confidentiality and integrity of the financial asset and sensitive information. For example, biometrics for extensive authentication. Therefore, MOT controls could have been implemented more precisely keeping labor and technical cost, efficiency and time in mind.

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

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

|  |  |  |  |
| --- | --- | --- | --- |
|  | Prevention | Resilience | Mixed |
| 2FA | 1000000 | 2500000 | 3000000 |
| VPN | 3000000 | 3250000 | 4000000 |
| DMZ | 2500000 | 3000000 | 4000000 |
| Redudant Server | 5500000 | 5750000 | 6000000 |
| Mirror Site | 2000000 | 3000000 | 4000000 |

Here residual risk reduction exceeds the budget for proposed controls.

**What is the (expected overall security risk reduction Benefit) / (proposed overall security risk budget Cost) ROI ratios for each of the 4 budgets in XIII?**

|  |  |  |
| --- | --- | --- |
| Implemented Controls | Cost | ROI |
| 2FA | 300000 | 12052.2 |
| VPN | 400000 | 8990.9625 |
| DMZ | 400000 | 9033.19375 |
| Redundant Server | 600000 | 6645.2125 |
| Mirror Site | 400000 | 8845.55625 |

**Do you recommend a Risk Prevention Strategy or a Risk Response Strategy or a combination such as a Risk reduction strategy or Risk ROI maximization Mixed Strategy?**

I would be more inclined towards Optimized Mixed Strategy. Although, Risk Prevention and Resilience strategy reduce the risk same or maybe more than mixed strategy, time and cost are the two aspects to be considered. Mixed strategy implements both Prevention and Response strategy at the same time. This can be important at a crucial time while identifying, managing, and mitigating threats and vulnerabilities. If the cost and efficiency proves out to be the same in both strategies, it depends on the organization which type of strategy to implement it according to their needs, infrastructures and exposure.