Amanda Bedard
IA 5200
Themis Papageorge
Spring 2019

HGA Risk Management

II. Table of Contents:

III. Executive Summary:

Information System Title:
Hypothetical Government Agency (HGA)

Information System Categorization:

Below Chart based on FIPS 199 Categorization

Information System Type	Impact Rating: Confidentiality	Impact Rating: Integrity	Impact Rating: Availability
Financial Resources	High	High	High
System Components	High	High	High
Personnel Information	High	High	Moderate
Contract Documents	High	High	Low
Internal Correspondence	High	High	High
Business Documents	High	High	Moderate
Memos and Reports	High	High	High

Information System Owner:

Name: Owen Sisteme
Title: CEO
Agency: HGA
Address: 11 Hypothetical St, Building 1, Fort Thomas, KY 41075
Email: o.sisteme@hga.gov
Phone: 859-123-4567

Authorizing Official:

Name: Arthur Rize
Title: Director of Operations
Agency: HGA
Address: 11 Hypothetical St, Building 1, Fort Thomas, KY 41075

Email: a.rize@hga.gov
Phone: 859-765-4321

Other Designated Contacts:

Name: Chelsea Inez-Oliver
Title: CIO
Agency: HGA
Address: 11 Hypothetical St, Building 1, Fort Thomas, KY 41075
Email: c.inez@hga.gov
Phone: 859-775-4422

Name: Ida Thomas
Title: IT Director
Agency: HGA
Address: 11 Hypothetical St, Building 2, Fort Thomas, KY 41075
Email: i.thomas@hga.gov
Phone: 859-965-1321

Assessment of Security Responsibility:

Name: Sergio Responbilli
Title: CSO
Agency: HGA
Address: 11 Hypothetical St, Building 3, Fort Thomas, KY 41075
Email: s.responbilli@hga.gov
Phone: 859-161-4321

Information System Operational Status:

Information System Type	**Operational Status**
Financial Resources	Operational
System Components	Major Modification
Personnel Information	Operational
Contract Documents	Operational
Internal Correspondence	Operational

Business Documents	Operational
Memos and Reports	Operational

Information System Type:

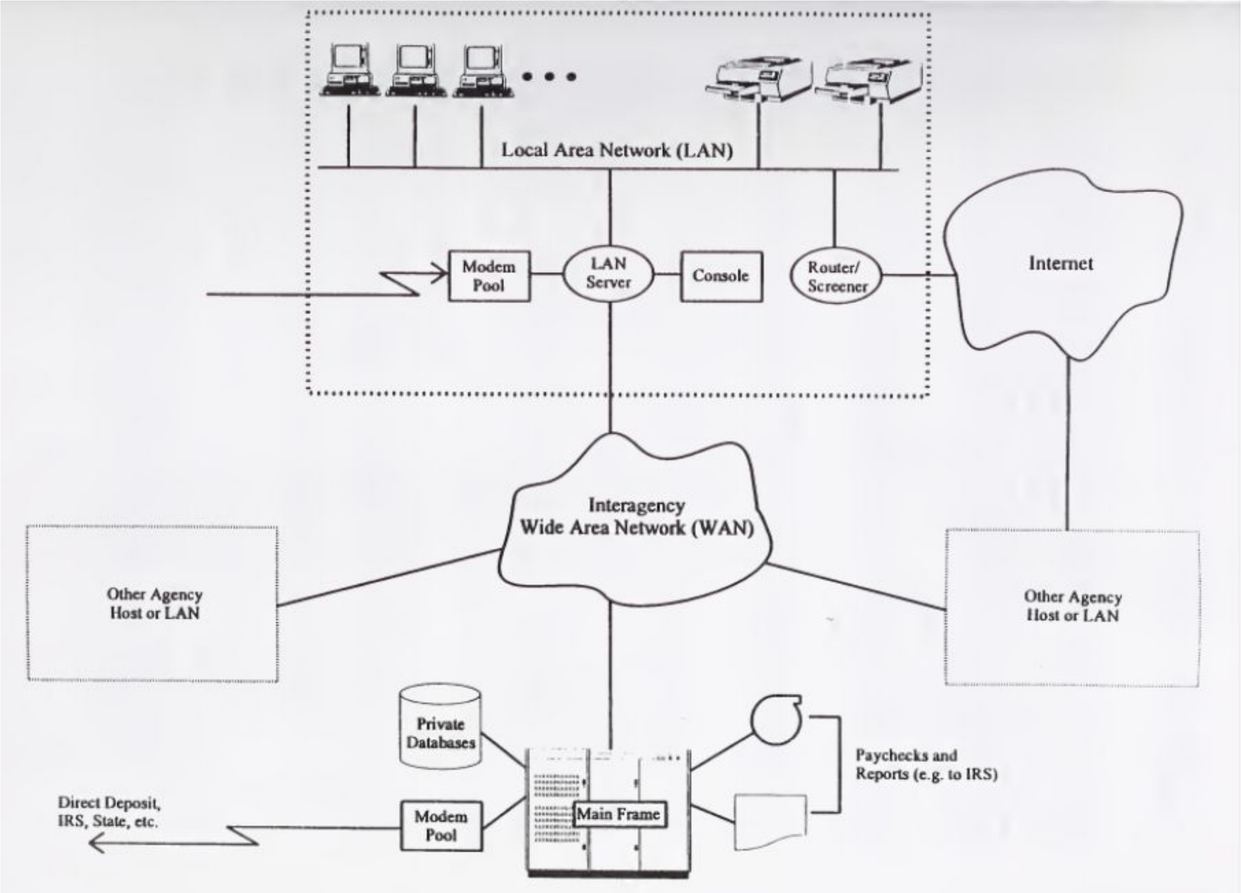
Major Application

General System Description/Purpose:

Hypothetical Government Agency (HGA) is a large government agency that works to ensure that those contracted by the government are paid correctly and accordingly. The functionality of this agency includes payroll for government employees, whether temporary/contract, part-time or full time, and contract negotiation.

System Environment:

Network Topology[1]:



[1] Diagram taken from source: https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-12.pdf. See appendix for full citation.

General Overview:

The system at HGA contains a Local Area Network (LAN) of user computers and printers, which feeds into a LAN Server. These resources are routed to the internet with a router/screener The LAN Server utilizes both a Modem Pool and Console for functionality, and feeds into a Wide Area Network (WAN) that is linked to a mainframe with private databases and other agency hosts/LANs. This can all be seen above in the diagram taken from the HGA documentation directly.

System Interconnections/Information Sharing:

System Name: Interagency Wide Area Network
Organization Type: Telecommunications Company
Agreement: ISA
Date: March 11, 2001
FIPS 199 Category: High
C&A Status: NIST Accredited
Auth Official: Sylvia Intercon

System Name: Mainframe
Organization Type: Federal Agency
Agreement: MOU
Date: March 19, 1989
FIPS 199 Category: High
C&A Status: NIST Accredited
Auth Official: Marianne Framme

Related Laws/Regulations/Policies[2]:

HGA would likely comply by the following regulations within the company and because of the nature of the information/data they are dealing with:

- *Fair Labor Standards Act (FLSA)*: This act is regarding overtime, equal pay, and hiring minors.
- *Federal Insurance Contributions Act (FICA)*: This act is regarding the retention of payroll records for 4 years and mandatory reporting.
- *Code of Federal Regulations (CFR)*: This code is regarding how to function as an agency of the US Government.
- *Electronic Funds Transfer Act (EFTA)*: An act regarding electronic fund transfers for those opting to receive pay through an electronic method.

[2] Section created using information from source: https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/usa. See appendix for full citation.

- *The Board of Governors of the Federal Reserve System (Federal Reserve)*: The central US banking structure who will likely be supervising the actions of HGA.

Minimum Security Controls:

Control	Implementation	Status	Control Type	Responsible Party
Policies - M1	Regular revision/creation of Policies	Partially Implemented	Common Control	CSO CISO
Program Management - M2	Having a structured computer/system security program	Partially Implemented	Common Control	CSO CISO
Risk Management- M3	Regular assessment and prevention of vulnerabilities	Not implemented	Common Control	CSO CISO
Life Cycle Planning- M4	An end to end lifecycle planned/implemented for all systems that require one	Partially Implemented	Common Control	CSO CISO
Assurance- M5	Assurance existing across all platforms including certification, testing, and cost considerations	Partially Implemented	Common Control	CISO
Personnel/User Issues- O1	Staffing and administration considerations	Implemented	Common Control	CSO CISO
Preparing for Contingencies and Disasters - O2	Planning and testing for a worst case	Partially Implemented	Common Control	CSO CISO
Incident Reporting and Handling- O3	Actions to be taken if an incident occurs	Not Implemented	Common Control	CSO CISO
Awareness, training, and education- O4	The training and awareness on efficient operation/ keeping safe in a digital world provided to staff	Partially Implemented	Common Control	CSO CISO

Security Considerations in Support and Operations- O5	How the operations team brings security into their day to day	Implemented	Common Control	CISO
Physical and Environmental Security- O6	The physical locks and boundaries protecting the assets	Partially Implemented	Common Control	CSO
Identification and Authentication- T1	The ability to accurately identify and authenticate a user	Implemented	Common Control	CISO
Logical Access Control- T2	Access control that makes sense for the user/scenario	Partially Implemented	Common Control	CSO CISO
Audit Trails- T3	Logging and storage of audit information with the systems	Partially Implemented	Common Control	CISO
Cryptography- T4	Proper encryption methodology applied to assets and data	Partially Implemented	Common Control	CISO

Information System Security Plan Complete Date:

February 3, 2019

Information System Security Plan Approval Date:

February 4, 2019

IV List of Assets with Values:

Assets Inventory:

Main Asset	**Sub Asset**	**Value (in US Dollar)**
A1: Financial Resources	-	1,000,000,000
A2: System Components	-	-
	A21: PCs	3,500,000
	A22: LAN Server	150,000
	A23: Router/Screener	200,000
	A24: Console	200,000
	A25: VPN Server	100,000
	A26: Printers	100,000
	A27: Dedicated Server	100,000
A3: Personnel Information	-	100,000,000
A4: Contracting and Procurement	-	1,000,000
A5: Draft Regulations	-	50,000
A6: Internal Correspondence	-	5,000,000
A7: Business Documents	-	5,000,000
A8: Reputation	-	Intangible
A9: Employee Confidence	-	Intangible

V. List of Threats:

Threats List:

Threat
T1: Payroll Fraud
T2: Payroll Errors
T3: Interruption of operations
T4: Disclosure or Brokerage of information
T5: Network-Related Attacks
T6: Other

VI. List of Vulnerabilities:

Security Vulnerability List:

Main Vulnerability Name	**Subcategory Name**
T1:V1: Vulnerabilities Related to Payroll Fraud	**V1.1**: Falsified Time Sheets
	V1.2: Unauthorized Access
	V1.3: Bogus Time and Attendance Applications
	V1.4: Unauthorized Modifications of Time and Attendance Sheets
T2:V2: Vulnerabilities Related to Payroll Errors	-
T3:V3: Vulnerabilities Related to Continuity of Operations	**V3.1**: COG Contingency Planning
	V3.2: Division Contingency Planning
	V3.3: Virus Prevention
	V3.4: Accidental Corruption and Loss of Data
T4:V4: Vulnerabilities Related to Disclosure or Brokerage of information	-
T5:V5: Vulnerabilities Related to Network-Related Attacks	-

VII. Threat/Vulnerability Pairs:

Threat/Vulnerability Pairs:

Threats:

- **T1**: Payroll Fraud
- **T2**: Payroll Errors
- **T3**: Interruption of operations
- **T5**: Network-Related Attacks

Vulnerabilities:

- **V1.3**: Bogus Time and Attendance Applications
- **V1.4**: Unauthorized Modifications of Time and Attendance Sheets
- **V3.4**: Accidental Corruption and Loss of Data
- **V5**: Vulnerabilities Related to Network-Related Attacks

Threat/Vulnerability Pairs:

	T1	**T2**	**T3**	**T5**
V1.3	5%	5%	1%	5%
V1.4	10%	5%	1%	2%
V3.4	5%	1%	5%	1%
V5	5%	1%	15%	5%

Risk Impact:

We assume 100% risk impact (0% resilience) to the assets, given that the vulnerabilities are exploited by the threats.

VIII. Assets Impacted by Threat/Vulnerability Pairs:

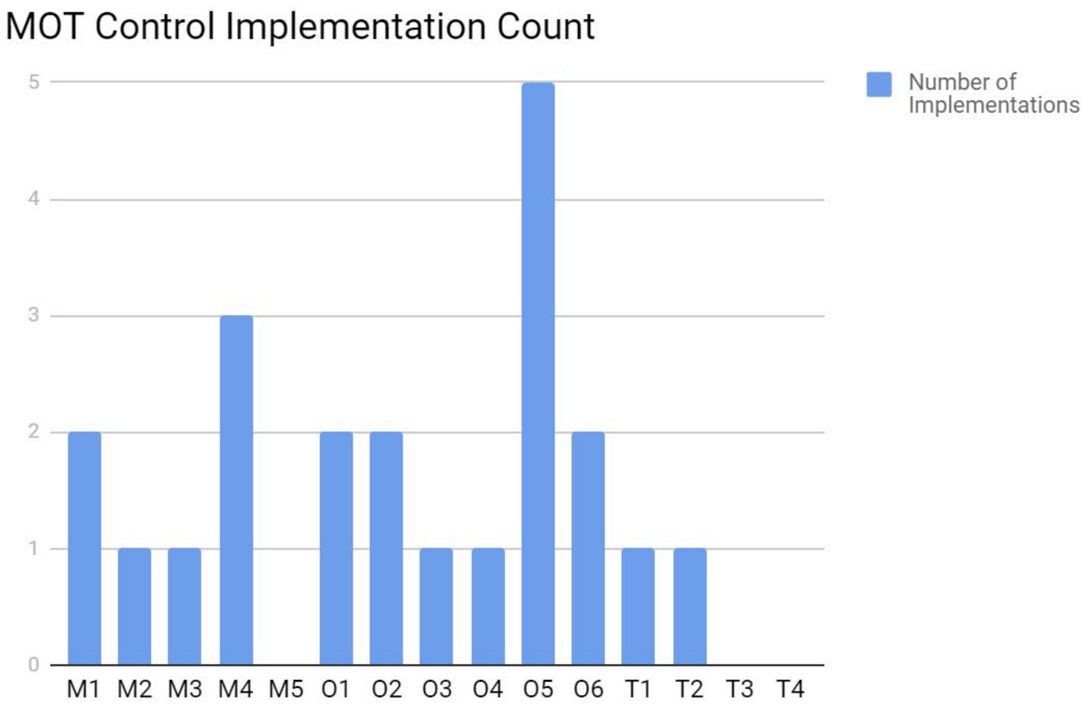
Asset	**Related Vulnerabilities**
A1: Financial Resources	**V1.3**: Bogus Time and Attendance Applications **V1.4**: Unauthorized Modifications of Time and Attendance Sheets **V3.4**: Accidental Corruption and Loss of Data **V5**: Vulnerabilities Related to Network-Related Attacks
A4: Contracting and Procurement	**V1.3**: Bogus Time and Attendance Applications **V1.4**: Unauthorized Modifications of Time and Attendance Sheets **V3.4**: Accidental Corruption and Loss of Data **V5**: Vulnerabilities Related to Network-Related Attacks
A6: Internal Correspondence	**V1.3**: Bogus Time and Attendance Applications **V1.4**: Unauthorized Modifications of Time and Attendance Sheets **V3.4**: Accidental Corruption and Loss of Data **V5**: Vulnerabilities Related to Network-Related Attacks
A21: PC’s	**V1.3**: Bogus Time and Attendance Applications **V1.4**: Unauthorized Modifications of Time and Attendance Sheets **V3.4**: Accidental Corruption and Loss of Data **V5**: Vulnerabilities Related to Network-Related Attacks

IX. MOT- Current Controls:

Existing Security Controls:

Main Existing Control Category	**Subcategory**	**MOT Controls**
EC1: General Use and Administration of HGA's Computer System	**EC1.1**: Access control	**T1, O1**
	EC1.2: Education of policies	**O4**
	EC1.3: Password Rotation/Management/Policies	**M1**
EC2: Protection Against Payroll Fraud and Errors (Time and Attendance Application)	**EC2.1**: Automated Processes	**O5**
	EC2.2: Data Validation	**O5**
	EC2.3: Centralization of Application	**O5**
	EC2.4: Data Backups with Digital Signatures	**O5, M4**
EC3: Protection Against Interruption of Operations	**EC3.1**: Division-Specific Contingency Plans	**M1, M2, M3, O3, O2**
	EC3.2: Communication Device Restriction	**O6**
	EC3.3: Regular patching/updating of systems	**O5, M4**
	EC3.4: Weekly Backup Requirement	**M4, O2**
	EC3.5: Hardware Backups Readily Available	**O6**
	EC3.6: Software install Restrictions	**T2, O1**

	EC3.7: Audit Logging/Reviews	
EC4: Protection Against Disclosure or Brokerage of Information	**EC4.1**: Physical, Procedural, and Automated Security Controls	**T3**
EC5: Protection Against Network-Related Threats	**EC5.1**: Traffic Filtering	**T2**
	EC5.2: Disallow Remote Sessions	**T2**
	EC5.3: Dial-In Restrictions	**T2**
EC6: Protection Against Risks from Non-HGA Computer Systems	**EC6.1**: Third-Party System Restrictions	**M3, T2**



The above histogram represents the MOT controls implemented across the systems with the existing controls in HGA

X. MOT- Controls Covered by Proposed Controls and VPN/DMZ Implementation:

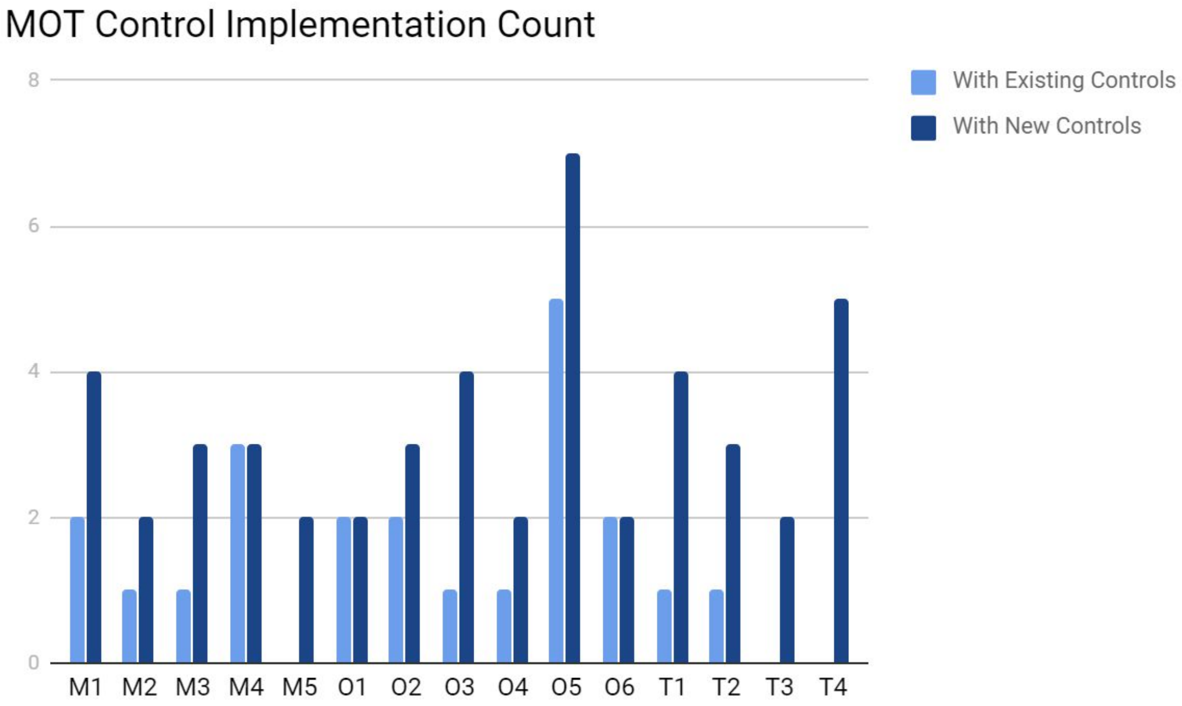
Proposed Controls (NC) and Controls Implemented with VPN/DMZ (VC):

Based on the 33 Cybersecurity Engineering principles, I recommend the following controls be implemented with the VPN/DMZ (listed in the chart):

- Use of key authentication instead of password
  - This involves storing a public/private key pair for anyone who wishes to use the server. This reduces the risk of a password attack, as well as further implement principle 15, as the users will not have to worry about remembering a password (and in turn, writing it down somewhere).
- Encryption in transit
  - This involves encrypting the data locally with (strong) encryption, sending through to the remote server, and then decrypting. This will help with principle 9, in covering the bases not already covered by existing controls.
- Audit logging
  - While HGA does implement SOME audit logging, they do not implement nearly enough. When introducing this VPN, they must ensure they are logging all traffic/interactions with the VPN, for principle 22.
- Lock the server in a room with limited access
  - This adds a layer of physical protection that the HGA has not been implementing a lot of, per principle 30.
- Implement a killswitch for the Internet
  - This will provide a quick way to shut off Internet access if an attack is being implemented. This will help cover principle 11, by protecting against one of the most likely places the attack will be coming from; the internet. It will also give the ability to stop an online attack in its tracks.

Main Proposed Control Category	**Subcategory**	**MOT Controls**
NC1: Controls Mitigating Vulnerabilities Related to Payroll Fraud	**NC1.1**: Server Administrative procedures and bugfixes	**O5**
	NC1.2: One time passwords	**M1**

	NC1.3: Digital signatures	**M5**
NC2: Controls Mitigating Payroll Error	-	**M3**
NC3: Controls Mitigating Vulnerabilities Related to Continuity of Operations	**NC3.1**: SETA	**O5, M2**
	NC3.2: Mainframe MOU	**T3, O3**
	NC3.3: Automated E-mail Reminders and Back-ups	**M3, M5, O5**
NC4: Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	**NC4.1**: Screen locks	**T1, T2**
	NC4.2: Hard Disk Encryption	**T4**
NC5: Controls Vulnerabilities Related to Network-Related Attacks	**NC5.1**: stronger I&A	**T1**
	NC5.2: Encrypting modems	**T4**
	NC5.3: Mainframe Communications Encryption	**T4**
VC1: Controls related to Data Protection	**VC1.1:** Key authentication	**T1, O3, T4**
	VC1.2: Encryption in transit	**T4**
VC2: Physical Access Controls	**VC2.1:** Lock the server in a room with limited access	**O2, T2**
VC3: Audit Controls	**VC3.1:** Audit logging of VPN/Server traffic	**M1, T3**
VC4: Reactive Controls	**VC4.1:** Internet killswitch	**M5, O3, O4**



The above histogram represents the implemented controls before and after the proposed controls and VPN implementation, light blue being before and dark blue being after.

XI. Security Risk Prevention Strategy (Current Controls):

Calculations of Assets with vulnerabilities discovered by new CISO and protected by current controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc.

Assets:

A1: Financial Resources - 1,000,000,000
A4: Contracting and Procurements - 1,000,000
A6: Internal Correspondence - 5,000,000
A21: PC's - 3,500,000

Threats:

T1: Payroll Fraud
T2: Payroll Errors
T3: Interruption of operations
T5: Network-Related Attacks

Vulnerabilities:

V1.3: Bogus Time and Attendance Applications
V1.4: Unauthorized Modifications of Time and Attendance Sheets
V3.4: Accidental Corruption and Loss of Data
V5: Vulnerabilities Related to Network-Related Attacks

Threat/Vulnerability Probability Calculations on Asset Subsets:

	T1	**T2**	**T3**	**T5**
V1.3	60%	65%	20%	35%
V1.4	70%	60%	15%	40%
V3.4	40%	70%	35%	55%
V5	50%	40%	55%	75%

Initial Risk:

We assume 100% risk impact (0% resilience) to the assets, given that the vulnerabilities are exploited by the threats.

Assets	T1* V1.3	T1* V1.4	T1* V3.4	T1 *V5	T2* V1.3	T2* V1.4	T2* V3.4	T2 *V5	T3* V1.3	T3* V1.4	T3* V3.4	T3 *V5	T5* V1.3	T5* V1.4	T5* V3.4	T5 *V5
A1	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%
A6	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A21	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Residual Risk Results:

Assets:

A1: 1,000,000,000 * (60% + 65% + 20% + 35% + 70% + 60% + 15% + 40% + 40% + 70% + 35% + 55% + 50% + 40% + 55% + 75%) = 9,110,000,000 > 1,000,000,000 (value of A1)
Risk = 1,000,000,000: Total Loss

A4: 1,000,000 * (60% + 65% + 20% + 35% + 70% + 60% + 15% + 40% + 40% + 70% + 35% + 55% + 50% + 40% + 55% + 75%) = 9,110,000 > 1,000,000 (value of A4)
Risk = 1,000,000: Total Loss

A6: 5,000,000 * (60% + 65% + 20% + 35% + 70% + 60% + 15% + 40% + 40% + 70% + 35% + 55% + 50% + 40% + 55% + 75%) = 45,550,000 > 5,000,000 (value of A7)
Risk = 5,000,000: Total Loss

A21: 3,500,000 * (60% + 65% + 20% + 35% + 70% + 60% + 15% + 40% + 40% + 70% + 35% + 55% + 50% + 40% + 55% + 75%) = 31,885,000 > 3,500,000 (value of A21)
Risk = 3,500,000: Total Loss

Total Residual Risk: $1,054,500,000

Vulnerabilities:

V1.3: 1,000,000,000 * (60% + 65% + 20% + 35%) + 1,000,000 * (60% + 65% + 20% + 35%) + 5,000,000 * (60% + 65% + 20% + 35%) + 3,500,000 * (60% + 65% + 20% + 35%) = $**1,817,100,000**

V1.4: 1,000,000,000 * (70% + 60% + 15% + 40%) + 1,000,000 * (70% + 60% + 15% + 40%) + 5,000,000 * (70% + 60% + 15% + 40%) + 3,500,000 * (70% + 60% + 15% + 40%) = $**1,867,575,000**

V3.4: 1,000,000,000 * (40% + 70% + 35% + 55%) + 1,000,000 * (40% + 70% + 35% + 55%) + 5,000,000 * (40% + 70% + 35% + 55%) + 3,500,000 * (40% + 70% + 35% + 55%)= $**2,019,000,000**

V5: 1,000,000,000 * (50% + 40% + 55% + 75%) + 1,000,000 * (50% + 40% + 55% + 75%) + 5,000,000 * (50% + 40% + 55% + 75%) + 3,500,000 * (50% + 40% + 55% + 75%) = $**2,220,900,000**

Residual Risk Ranking:

Assets:

1: A1
2: A6
3: A21
4: A4

Vulnerabilities:

1: V5
2: V3.4
3: V1.4
4: V1.3

XII. Security Risk Prevention Strategy (New Control Implementation):

Calculations of Assets with vulnerabilities discovered by new CISO and protected by current and proposed by new CISO controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking of which vulnerability should be addressed by controls first, second, third etc

Assets:

A1: Financial Resources - 1,000,000,000
A4: Contracting and Procurements - 1,000,000
A6: Internal Correspondence - 5,000,000
A21: PC's - 3,500,000

Threats:

T1: Payroll Fraud
T2: Payroll Errors
T3: Interruption of operations
T5: Network-Related Attacks

Vulnerabilities:

V1.3: Bogus Time and Attendance Applications
V1.4: Unauthorized Modifications of Time and Attendance Sheets
V3.4: Accidental Corruption and Loss of Data
V5: Vulnerabilities Related to Network-Related Attacks

Threat/Vulnerability Pairs:

	T1	**T2**	**T3**	**T5**
V1.3	50%	45%	10%	25%
V1.4	60%	50%	10%	30%
V3.4	30%	60%	25%	45%
V5	40%	30%	35%	55%

Initial Risk:

We assume 100% risk impact (0% resilience) to the assets, given that the vulnerabilities are exploited by the threats.

Assets	T1* V1.3	T1* V1.4	T1* V3.4	T1 *V5	T2* V1.3	T2* V1.4	T2* V3.4	T2 *V5	T3* V1.3	T3* V1.4	T3* V3.4	T3 *V5	T5* V1.3	T5* V1.4	T5* V3.4	T5 *V5
A1	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%
A6	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A21	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Residual Risk Results:

Assets:

A1: 1,000,000,000 * (50% + 45% + 10% + 25% + 60% + 50% + 10% + 30% + 30% + 60% + 25% + 45% + 40% + 30% + 35% + 55%) = 6,000,000,000 > 1,000,000,000 (value of A1)
Risk = 1,000,000,000: Total Loss

A4: 1,000,000 * (50% + 45% + 10% + 25% + 60% + 50% + 10% + 30% + 30% + 60% + 25% + 45% + 40% + 30% + 35% + 55%) = 6,000,000 > 1,000,000 (value of A4)
Risk = 1,000,000: Total Loss

A6: 5,000,000 * (50% + 45% + 10% + 25% + 60% + 50% + 10% + 30% + 30% + 60% + 25% + 45% + 40% + 30% + 35% + 55%) = 30,000,000 > 5,000,000 (value of A7)
Risk = 5,000,000: Total Loss

A21: 3,500,000 * (50% + 45% + 10% + 25% + 60% + 50% + 10% + 30% + 30% + 60% + 25% + 45% + 40% + 30% + 35% + 55%) = 21,000,000 > 3,500,000 (value of A21)
Risk = 3,500,000: Total Loss

Total Residual Risk: $1,054,500,000

Risk Due to Vulnerabilities:

V1.3: 1,000,000,000 * (50% + 45% + 10% + 25%) + 1,000,000 * (50% + 45% + 10% + 25%) + 5,000,000 * (50% + 45% + 10% + 25%) + 3,500,000 * (50% + 45% + 10% + 25%) = $**1,312,350,000**

V1.4: 1,000,000,000 * (60% + 50% + 10% + 30%) + 1,000,000 * (60% + 50% + 10% + 30%) + 5,000,000 * (60% + 50% + 10% + 30%) + 3,500,000 * (60% + 50% + 10% + 30%) = $**1,514,250,000**

V3.4: 1,000,000,000 * (30% + 60% + 25% + 45%) + 1,000,000 * (30% + 60% + 25% + 45%) + 5,000,000 * (30% + 60% + 25% + 45%) + 3,500,000 * (30% + 60% + 25% + 45%)= $**1,615,200,000**

V5: 1,000,000,000 * (40% + 30% + 35% + 55%) + 1,000,000 * (40% + 30% + 35% + 55%) + 5,000,000 * (40% + 30% + 35% + 55%) + 3,500,000 * (40% + 30% + 35% + 55%) = $**1,615,200,000**

Residual Risk Ranking:

Assets:

1: A1
2: A6
3: A21
4: A4

Vulnerabilities:

1: V5 & V3.4
2: V1.4
3: V1.3

XIII. Security Risk Prevention Strategy (Protected by current, new, and missing MOT Controls):

Calculations of Assets with vulnerabilities discovered by new CISO and protected by current and proposed by new CISO controls and non-covered/missing MOT controls. Calculate residual risks for assets and total HGA residual risk. Calculate vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc. Compare HGA current, CISO proposed, and VPN and DMZ risk controls to the 157 risk controls from Common Criteria.

Assets:

A1: Financial Resources - 1,000,000,000
A4: Contracting and Procurements - 1,000,000
A6: Internal Correspondence - 5,000,000
A21: PC's - 3,500,000

Threats:

T1: Payroll Fraud
T2: Payroll Errors
T3: Interruption of operations
T5: Network-Related Attacks

Vulnerabilities:

V1.3: Bogus Time and Attendance Applications
V1.4: Unauthorized Modifications of Time and Attendance Sheets
V3.4: Accidental Corruption and Loss of Data
V5: Vulnerabilities Related to Network-Related Attacks

Existing and New Security Controls:

Main Existing Control Category	Subcategory	MOT Controls
EC1: General Use and Administration of HGA's Computer System	**EC1.1**: Access control	**T1, O1**
	EC1.2: Education of policies	**O4**
	EC1.3: Password Rotation/Management/Policies	**M1**

EC2: Protection Against Payroll Fraud and Errors (Time and Attendance Application)	**EC2.1**: Automated Processes	**O5**
	EC2.2: Data Validation	**O5**
	EC2.3: Centralization of Application	**O5**
	EC2.4: Data Backups with Digital Signatures	**O5, M4**
EC3: Protection Against Interruption of Operations	**EC3.1**: Division-Specific Contingency Plans	**M1, M2, M3, O3, O2**
	EC3.2: Communication Device Restriction	**O6**
	EC3.3: Regular patching/updating of systems	**O5, M4**
	EC3.4: Weekly Backup Requirement	**M4, O2**
	EC3.5: Hardware Backups Readily Available	**O6**
	EC3.6: Software install Restrictions	**T2, O1**
	EC3.7: Audit Logging/Reviews	**T3**
EC4: Protection Against Disclosure or Brokerage of Information	**EC4.1**: Physical, Procedural, and Automated Security Controls	**T2**
EC5: Protection Against Network-Related Threats	**EC5.1**: Traffic Filtering	**T2**
	EC5.2: Disallow Remote Sessions	**T2**
	EC5.3: Dial-In Restrictions	**T2**
EC6: Protection Against Risks from Non-HGA Computer Systems	**EC6.1**: Third-Party System Restrictions	**M3, T2**
NC1: Controls Mitigating	**NC1.1**: Server Administrative	**O5**

Vulnerabilities Related to Payroll Fraud	procedures and bugfixes	
	NC1.2: One time passwords	**M1**
	NC1.3: Digital signatures	**M5**
NC2: Controls Mitigating Payroll Error	-	**M3**
NC3: Controls Mitigating Vulnerabilities Related to Continuity of Operations	**NC3.1**: SETA	**O5, M2**
	NC3.2: Mainframe MOU	**T3, O3**
	NC3.3: Automated E-mail Reminders and Back-ups	**M3, M5, O5**
NC4: Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	**NC4.1**: Screen locks	**T1, T2**
	NC4.2: Hard Disk Encryption	**T4**
NC5: Controls Vulnerabilities Related to Network-Related Attacks	**NC5.1**: stronger I&A	**T1**
	NC5.2: Encrypting modems	**T4**
	NC5.3: Mainframe Communications Encryption	**T4**

It appears that the following Risk Management Controls are missing/lacking presence in the table:

- M1: Policies
- M2: Program Management
- M3: Risk Management
- O1: Personnel/User Issues
- O2: Preparing for Contingencies and Disasters
- O3: Incident Reporting and Handling
- O4: Awareness, Training, and Education
- O6: Physical and Environmental Security
- T3: Audit Trails

HGA needs to spend more time on management and operation if they wish to have a fully secure infrastructure. Many of the attack types that are associated with the vulnerabilities listed in the subset (especially V3.4) can be almost entirely reduced by a mix of solid controls and good user training/awareness.

Threat/Vulnerability Pairs:

	T1	**T2**	**T3**	**T5**
V1.3	5%	5%	1%	5%
V1.4	10%	5%	1%	2%
V3.4	5%	1%	5%	1%
V5	5%	1%	10%	15%

Common Criteria Comparison[3]:

While at this point in the analysis, HGA has implemented a decent number of the Common Criteria standards, it is clear they are not all fully covered by the agency, which is, overall, still carrying a fairly basic security plan. A few notable mentions on topics and policies from the Common Criteria list are:

- *Awareness and training*: HGA has SOME awareness and training methodologies implemented, but nowhere near enough to fulfill all the AT categories in the Common Criteria
- *Incident Response*: HGA has almost no training or exercises regarding incident response, leaving gaps at IR-2: Incident Response Training and IR-3: Incident Response Testing and Exercises among others.
- *System and Communications Protection*: While the basics are there for HGA, they are notably missing a few of the more advanced topics, such as SC-26: Honeypots and many key topics such as SC-12: Cryptographic Key Establishment and Management

Initial Risk:

We assume 100% risk impact (0% resilience) to the assets, given that the vulnerabilities are exploited by the threats.

Assets	**T1* V1.3**	**T1* V1.4**	**T1* V3.4**	**T1 *V5**	**T2* V1.3**	**T2* V1.4**	**T2* V3.4**	**T2 *V5**	**T3* V1.3**	**T3* V1.4**	**T3* V3.4**	**T3 *V5**	**T5* V1.3**	**T5* V1.4**	**T5* V3.4**	**T5 *V5**
A1	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

[3] Section created using resources from source: https://www.commoncriteriaportal.org/ccra/index.cfm. See appendix for full citation.

A4	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A6	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A21	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Residual Risk Results:

Assets:

A1: 1,000,000,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 10% + 15%) = 770,000,000 < 1,000,000,000 (value of A1)
Risk = 770,000,000: Partial Loss

A4: 1,000,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 10% + 15%) = 770,000 < 1,000,000 (value of A4)
Risk = 770,000: Partial Loss

A6: 5,000,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 10% + 15%) = 3,850,000 < 5,000,000 (value of A6)
Risk = 3,850,000: Partial Loss

A21: 3,500,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 10% + 15%) = 2,695,000 < 3,500,000 (value of A21)
Risk = 2,695,000: Partial Loss

Total Residual Risk: $777,315,000

Vulnerabilities:

V1.3: 1,000,000,000 * (5% + 5% + 1% + 5%) + 1,000,000 * (5% + 5% + 1% + 5%) + 5,000,000 * (5% + 5% + 1% + 5%) + 3,500,000 * (5% + 5% + 1% + 5%) = $**161,520,000**

V1.4: 1,000,000,000 * (10% + 5% + 1% + 2%) + 1,000,000 * (10% + 5% + 1% + 2%) + 5,000,000 * (10% + 5% + 1% + 2%) + 3,500,000 * (10% + 5% + 1% + 2%) = $**181,710,000**

V3.4: 1,000,000,000 * (5% + 1% + 5% + 1%) + 1,000,000 * (5% + 1% + 5% + 1%) + 5,000,000 * (5% + 1% + 5% + 1%) + 3,500,000 * (5% + 1% + 5% + 1%)= $**121,140,000**

V5: 1,000,000,000 * (5% + 1% + 10% + 15%) + 1,000,000 * (5% + 1% + 10% + 15%) + 5,000,000 * (5% + 1% + 10% + 15%) + 3,500,000 * (5% + 1% + 10% + 15%) = $**312,945,000**

Residual Risk Ranking:

Assets:

1: A1
2: A6
3: A21
4: A4

Vulnerabilities:

1: V5
2: V1.4
3: V1.3
4: V3.4

XIV. Security Risk Prevention Strategy (Including VPN):

Calculations of Assets with VPN and DMZ controls. Calculate for a Security Risk Prevention Strategy, and a Security Risk Response (Resilience) Strategy, and a Mixed (combination of the two) Strategy residual risks for assets and total HGA residual risk, vulnerability risks for ranking which vulnerability should be addressed by controls first, second, third etc.

Existing Security Controls:

Main Existing Control Category	**Subcategory**	**MOT Controls**
EC1: General Use and Administration of HGA's Computer System	**EC1.1**: Access control	**T1, O1**
	EC1.2: Education of policies	**O4**
	EC1.3: Password Rotation/Management/Policies	**M1**
EC2: Protection Against Payroll Fraud and Errors (Time and Attendance Application)	**EC2.1**: Automated Processes	**O5**
	EC2.2: Data Validation	**O5**
	EC2.3: Centralization of Application	**O5**
	EC2.4: Data Backups with Digital Signatures	**O5, M4**
EC3: Protection Against Interruption of Operations	**EC3.1**: Division-Specific Contingency Plans	**M1, M2, M3, O3, O2**
	EC3.2: Communication Device Restriction	**O6**
	EC3.3: Regular patching/updating of systems	**O5, M4**
	EC3.4: Weekly Backup Requirement	**M4, O2**
	EC3.5: Hardware Backups	**O6**

	Readily Available	
	EC3.6: Software install Restrictions	**T2, O1**
	EC3.7: Audit Logging/Reviews	
EC4: Protection Against Disclosure or Brokerage of Information	**EC4.1**: Physical, Procedural, and Automated Security Controls	**T3**
EC5: Protection Against Network-Related Threats	**EC5.1**: Traffic Filtering	**T2**
	EC5.2: Disallow Remote Sessions	**T2**
	EC5.3: Dial-In Restrictions	**T2**
EC6: Protection Against Risks from Non-HGA Computer Systems	**EC6.1**: Third-Party System Restrictions	**M3, T2**

Proposed Controls (NC) and Controls Implemented with VPN/DMZ (VC):

Main Proposed Control Category	**Subcategory**	**MOT Controls**
NC1: Controls Mitigating Vulnerabilities Related to Payroll Fraud	**NC1.1**: Server Administrative procedures and bugfixes	**O5**
	NC1.2: One time passwords	**M1**
	NC1.3: Digital signatures	**M5**
NC2: Controls Mitigating Payroll Error	-	**M3**
NC3: Controls Mitigating Vulnerabilities Related to Continuity of Operations	**NC3.1**: SETA	**O5, M2**
	NC3.2: Mainframe MOU	**T3, O3**
	NC3.3: Automated E-mail	**M3, M5, O5**

	Reminders and Back-ups	
NC4: Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	**NC4.1**: Screen locks	**T1, T2**
	NC4.2: Hard Disk Encryption	**T4**
NC5: Controls Vulnerabilities Related to Network-Related Attacks	**NC5.1**: stronger I&A	**T1**
	NC5.2: Encrypting modems	**T4**
	NC5.3: Mainframe Communications Encryption	**T4**
VC1: Controls related to Data Protection	**VC1.1:** Key authentication	**T1, O3, T4**
	VC1.2: Encryption in transit	**T4**
VC2: Physical Access Controls	**VC2.1:** Lock the server in a room with limited access	**O2, T2**
VC3: Audit Controls	**VC3.1:** Audit logging of VPN/Server traffic	**M1, T3**
VC4: Reactive Controls	**VC4.1:** Internet killswitch	**M5, O3, O4**

Assets:

- **A1**: Financial Resources - 1,000,000,000
- **A4**: Contracting and Procurements - 1,000,000
- **A6**: Internal Correspondence - 5,000,000
- **A21**: PC's - 3,500,000
- **A25**: VPN Server
- **A27**: Dedicated Server

Threat/Vulnerability Pairs:

Threats:

- **T1**: Payroll Fraud
- **T2**: Payroll Errors
- **T3**: Interruption of operations
- **T5**: Network-Related Attacks

Vulnerabilities:

- **V1.3**: Bogus Time and Attendance Applications
- **V1.4**: Unauthorized Modifications of Time and Attendance Sheets
- **V3.4**: Accidental Corruption and Loss of Data
- **V5**: Vulnerabilities Related to Network-Related Attacks

Threat/Vulnerability Pairs (Updated with new assets):

	T1	**T2**	**T3**	**T5**
V1.3	5%	5%	1%	5%
V1.4	10%	5%	1%	2%
V3.4	5%	1%	5%	1%
V5	5%	1%	15%	5%

Initial Risk:

We assume 100% risk impact (0% resilience) to the assets, given that the vulnerabilities are exploited by the threats.

Assets	**T1* V1.3**	**T1* V1.4**	**T1* V3.4**	**T1 *V5**	**T2* V1.3**	**T2* V1.4**	**T2* V3.4**	**T2 *V5**	**T3* V1.3**	**T3* V1.4**	**T3* V3.4**	**T3 *V5**	**T5* V1.3**	**T5* V1.4**	**T5* V3.4**	**T5 *V5**
A1	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%
A6	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A21	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Residual Risk Results:

Assets:

A1: 1,000,000,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 15% + 5%) = 770,000,000 < 1,000,000,000 (value of A1)
Risk = 720,000,000: Partial Loss

A4: 1,000,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 15% + 5%) = 770,000 < 1,000,000 (value of A4)
Risk = 720,000: Partial Loss

A6: 5,000,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 15% + 5%) = 3,850,000 < 5,000,000 (value of A6)
Risk = 3,600,000: Partial Loss

A21: 3,500,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 10% + 15%) = 2,520,000 < 3,500,000 (value of A21)
Risk = 2,520,000: Partial Loss

A25: 100,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 10% + 15%) = 77,000 < 100,000 (value of A21)
Risk = 77,000: Partial Loss

A27: 100,000 * (5% + 5% + 1% + 5% + 10% + 5% + 1% + 2% + 5% + 1% + 5% + 1% + 5% + 1% + 10% + 15%) = 77,000 < 100,000 (value of A21)
Risk = 77,000: Partial Loss

Total Residual Risk: $726,994,000

Risk Due to Vulnerabilities:

V1.3: 1,000,000,000 * (5% + 5% + 1% + 5%) + 1,000,000 * (5% + 5% + 1% + 5%) + 5,000,000 * (5% + 5% + 1% + 5%) + 3,500,000 * (5% + 5% + 1% + 5%) + 100,000 * (5% + 5% + 1% + 5%) + 100,000 * (5% + 5% + 1% + 5%) = $**161,552,000**

V1.4: 1,000,000,000 * (10% + 5% + 1% + 2%) + 1,000,000 * (10% + 5% + 1% + 2%) + 5,000,000 * (10% + 5% + 1% + 2%) + 3,500,000 * (10% + 5% + 1% + 2%) + 100,000 * (10% + 5% + 1% + 2%) + 100,000 * (10% + 5% + 1% + 2%) = $**181,746,000**

V3.4: 1,000,000,000 * (5% + 1% + 5% + 1%) + 1,000,000 * (5% + 1% + 5% + 1%) + 5,000,000 * (5% + 1% + 5% + 1%) + 3,500,000 * (5% + 1% + 5% + 1%) + 100,000 * (5% + 1% + 5% + 1%) + 100,000 * (5% + 1% + 5% + 1%)= $**121,164,000**

V5: 1,000,000,000 * (5% + 1% + 15% + 5%) + 1,000,000 * (5% + 1% + 15% + 5%) + 5,000,000 * (5% + 1% + 15% + 5%) + 3,500,000 * (5% + 1% + 15% + 5%) + 1,000,000 * (5% + 1% + 15% + 5%) + 1,000,000 * (5% + 1% + 15% + 5%) = $**262,522,000**

Residual Risk Ranking:

Assets:

1: A1
2: A6
3: A21

4: A4
5: A25 & A27

Vulnerabilities:

1: V5
2: V1.4
3: V1.3
4: V3.4

Threat/Vulnerability Pairs (Updated with Preventive and Response strategy):

	T1	T2	T3	T5
V1.3	5%	5%	1%	1%
V1.4	5%	5%	1%	2%
V3.4	5%	1%	1%	1%
V5	5%	1%	1%	2%

With a mixed strategy, we will see a decent drop in what is already a fairly low percentage quantity. We will also see the values for T3, Interruption of operations drop to almost nothing, as a good responsive strategy ensures that there is minimal to no impact on operations. Another field that has seen a significant drop is Network related threats, as covering many bases both preventive and responsively will make it harder for the attacker to be successful and reduce the impact of a successful attack. As the first two threats are likely internal/dependent on the end user, they saw much less reduction.

Initial Risk:

We assume 100% risk impact (0% resilience) to the assets, given that the vulnerabilities are exploited by the threats.

Assets	T1* V1.3	T1* V1.4	T1* V3.4	T1 *V5	T2* V1.3	T2* V1.4	T2* V3.4	T2 *V5	T3* V1.3	T3* V1.4	T3* V3.4	T3 *V5	T5* V1.3	T5* V1.4	T5* V3.4	T5 *V5
A1	100%	100%	100%	100%	100%	100%	100%	100%	50%	50%	10%	10%	100%	100%	100%	100%
A4	100%	100%	100%	100%	100%	100%	100%	100%	10%	10%	10%	10%	10%	10%	10%	10%
A6	50%	50%	50%	50%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A21	50%	50%	50%	50%	100%	100%	100%	100%	10%	10%	10%	10%	100%	100%	100%	100%

Residual Risk Results:

Assets:

A1: 1,000,000,000 * (5% + 5% + 1% + 1% + 5% + 5% + 1% + 2% + 5% + 1% + 1% + 1% + 5% + 1% + 1% + 2%) = 420,000,000 < 1,000,000,000 (value of A1)
Risk = 420,000,000: Partial Loss

A4: 1,000,000 * (5% + 5% + 1% + 1% + 5% + 5% + 1% + 2% + 5% + 1% + 1% + 1% + 5% + 1% + 1% + 2%) = 420,000 < 1,000,000 (value of A4)
Risk = 420,000: Partial Loss

A6: 5,000,000 * (5% + 5% + 1% + 1% + 5% + 5% + 1% + 2% + 5% + 1% + 1% + 1% + 5% + 1% + 1% + 2%) = 2,100,000 < 5,000,000 (value of A6)
Risk = 2,100,000: Partial Loss

A21: 3,500,000 * (5% + 5% + 1% + 1% + 5% + 5% + 1% + 2% + 5% + 1% + 1% + 1% + 5% + 1% + 1% + 2%) = 1,470,000 < 3,500,000 (value of A21)
Risk = 1,470,000: Partial Loss

A25: 100,000 * (5% + 5% + 1% + 1% + 5% + 5% + 1% + 2% + 5% + 1% + 1% + 1% + 5% + 1% + 1% + 2%) = 77,000 < 100,000 (value of A21)
Risk = 42,000: Partial Loss

A27: 100,000 * (5% + 5% + 1% + 1% + 5% + 5% + 1% + 2% + 5% + 1% + 1% + 1% + 5% + 1% + 1% + 2%) = 77,000 < 100,000 (value of A21)
Risk = 42,000: Partial Loss

Total Residual Risk: $424,074,000

Risk Due to Vulnerabilities:

V1.3: 1,000,000,000 * (5% + 5% + 1% + 1%) + 1,000,000 * (5% + 5% + 1% + 1%) + 5,000,000 * (5% + 5% + 1% + 1%) + 3,500,000 * (5% + 5% + 1% + 1%) + 100,000 * (5% + 5% + 1% + 1%) + 100,000 * (5% + 5% + 1% + 1%) = $**121,164,000**

V1.4: 1,000,000,000 * (5% + 5% + 1% + 2%) + 1,000,000 * (5% + 5% + 1% + 2%) + 5,000,000 * (5% + 5% + 1% + 2%) + 3,500,000 * (5% + 5% + 1% + 2%) + 100,000 * (5% + 5% + 1% + 2%) + 100,000 * (5% + 5% + 1% + 2%) = $**131,261,000**

V3.4: 1,000,000,000 * (5% + 1% + 1% + 1%) + 1,000,000 * (5% + 1% + 1% + 1%) + 5,000,000 * (5% + 1% + 1% + 1%) + 3,500,000 * (5% + 1% + 1% + 1%) + 100,000 * (5% + 1% + 1% + 1%) + 100,000 * (5% + 1% + 1% + 1%)= $**80,776,000**

V5: 1,000,000,000 * (5% + 1% + 1% + 2%) + 1,000,000 * (5% + 1% + 1% + 2%) + 5,000,000 * (5% + 1% + 1% + 2%) + 3,500,000 * (5% + 1% + 1% + 2%) + 1,000,000 * (5% + 1% + 1% + 2%) + 1,000,000 * (5% + 1% + 1% + 2%) = $**90,873,000**

Residual Risk Ranking:

Assets:

1: A1
2: A6
3: A21
4: A4
5: A25 & A27

Vulnerabilities:

1: V1.4
2: V1.3
3: V5
4: V3.4

XV. Conclusion:

Conclusion:

As demonstrated in sections XI to XIV, Hypothetical Government Agency (HGA) began their security journey with very limited controls and a very high level of risk for the systems included in the calculations. With the proposed CISO controls, and introduction of the VPN and DMZ controls, those numbers have reduced drastically, and HGA has minimally addressed every MOT control on the list (which can be seen in the histogram in section X). While some of the MOT controls are not heavily covered with this plan, it is a good start for HGA, where they can implement these controls and see the benefits over time, which may also (as a secondary effect) lead to reduced maintenance costs (with controls such as automation) and a more efficient workflow (due to clearer defined processes and better trained users) that will essentially pay for this effort.

HGA should focus on implementing a combined strategy for optimal return of investment, as risk response controls have the added ability of reducing the time and effort put into responding and recovering from an attack and risk prevention has the added secondary effects mentioned above, such as better trained users, smoother processes, and maintenance cost reduction.

Proposed Budget:

The proposed starting budget for Hypothetical Government Agency (HGA)'s expenditure into security is a **$34.3 Million pool distributed over 5 years**.

Implementing the VPN/DMZ will result in annual cost savings that can be contributed to this pool, and considering the large size and high value of HGA, $34.3 Million is only a fraction (less than 0.005%) of their financial resources asset, the highest value asset in their ownership. How this money is distributed will be pending which initiatives HGA decides to tackle first. The duration of this budget is intended to give HGA incentive for an ongoing security initiative, and a pool that can change/grow with the savings these controls will implement, as HGA start to see results as they implement controls and policies that will hopefully become standard across the Agency. The total pool takes into account that all the controls are implemented in the first year, and maintained until year 5.

Main Proposed Control Category	**Estimated Cost To Implement (year 1) and Maintain (Dollars)**
NC1: Controls Mitigating Vulnerabilities Related to Payroll Fraud	**500,000 + 500,000/yr**
NC2: Controls Mitigating Payroll Error	**1,000,000 + 500,000/yr**
NC3: Controls Mitigating Vulnerabilities Related to Continuity of Operations	**2,000,000 + 1,000,000/yr**

NC4: Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	**2,000,000 + 500,000/yr**
NC5: Controls Vulnerabilities Related to Network-Related Attacks	**1,000,000 + 500,000/yr**
VC1: Controls related to Data Protection	**200,000 + 100,000/yr**
VC2: Physical Access Controls	**500,000 + 500,000/yr**
VC3: Audit Controls	**200,000 + 100,000/yr**
VC4: Reactive Controls	**1,000,000 + 500,000/yr**

As can be seen in the calculation sections, moving from current controls Residual Risk to the new implementation with all controls/VPN/DMZ implementation with a combined resilience and preventive strategy will reduce the residual risk by the following:

$1,054,500,000 - $424,074,000 = $630,426,000

Which is much greater than the $34,300,000 requested for the five-year initiative.

Ratio: 34,300,000 / 630,426,000 = 0.05440765

XVI. Appendix:

Works Cited:

Nieles, M., Dempsey, K., & Pillitteri, V. Y. (1995, October). An Introduction to Computer Security: The NIST Handbook. Retrieved January 28, 2019, from https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-12.pdf

Sahni, R., & Byrne, T. J. (2018). Banking Regulation 2018 | USA | Laws and Regulations - Global Legal Insights. Retrieved February 3, 2019, from https://www.globallegalinsights.com/practice-areas/banking-and-finance-laws-and-regulations/usa

The Common Criteria. (n.d.). About The Common Criteria. Retrieved February 3, 2019, from https://www.commoncriteriaportal.org/ccra/index.cfm