Risk Management Plan for Hypothetical Government Agency (HGA)

Abhishek Ningala

Security Risk Management and Assessment (IA5200)

Themis A Papageorge

October 6, 2019

Contents

III. Executive Summary

1. Information System Name / Title:

   Hypothetical Government Agency (HGA)

2. Information System Categorization

Information System Asset	Impact		
	Confidentiality	Integrity	Availability
Financial Resources	High	High	High
System Components	High	High	High
Personnel Information	High	High	High
Contracting and Procurement Documents	High	High	High
Draft Regulations	High	High	High
Internal Correspondence	High	High	High
Business Documents	High	High	High

The overall value is High.

3. Information System Owner

   Name: Dennis R Sterling
   Title: Chief Information Officer
   Agency: Hypothetical Government Agency (HGA)
   Address: 4580 Aspen Court, Boston, MA
   Email Address: dennis.s@gmail.com
   Phone Number: 617-368-2898

4. Authorizing Official

   Name: Sophia C Thompson
   Title: Chief Security Officer
   Agency: Hypothetical Government Agency (HGA)
   Address: 4546 Rainy Day Drive, Boston, MA
   Email Address: sophia.t@gmail.com
   Phone Number: 617-937-5169

5. Other Designated Contacts

Name: Jean J pears
Title: Information Director
Agency: Hypothetical Government Agency (HGA)
Address: 3905 Aspen Court, Boston, MA
Email Address: Jean.jsp@gmail.com
Phone Number: 617-369-1223

6. Assignment of Security Responsibility

Name: Christopher N Jenn
Title: Chief Information Security Officer
Agency: Hypothetical Government Agency (HGA)
Address: 559 Doctors Drive, Boston, MA
Email Address: jenn.chris@gmail.com
Phone Number: 617-828-1496

7. Information System Operational Status

The status of information system operational status of HGA is operational.

8. Information System type

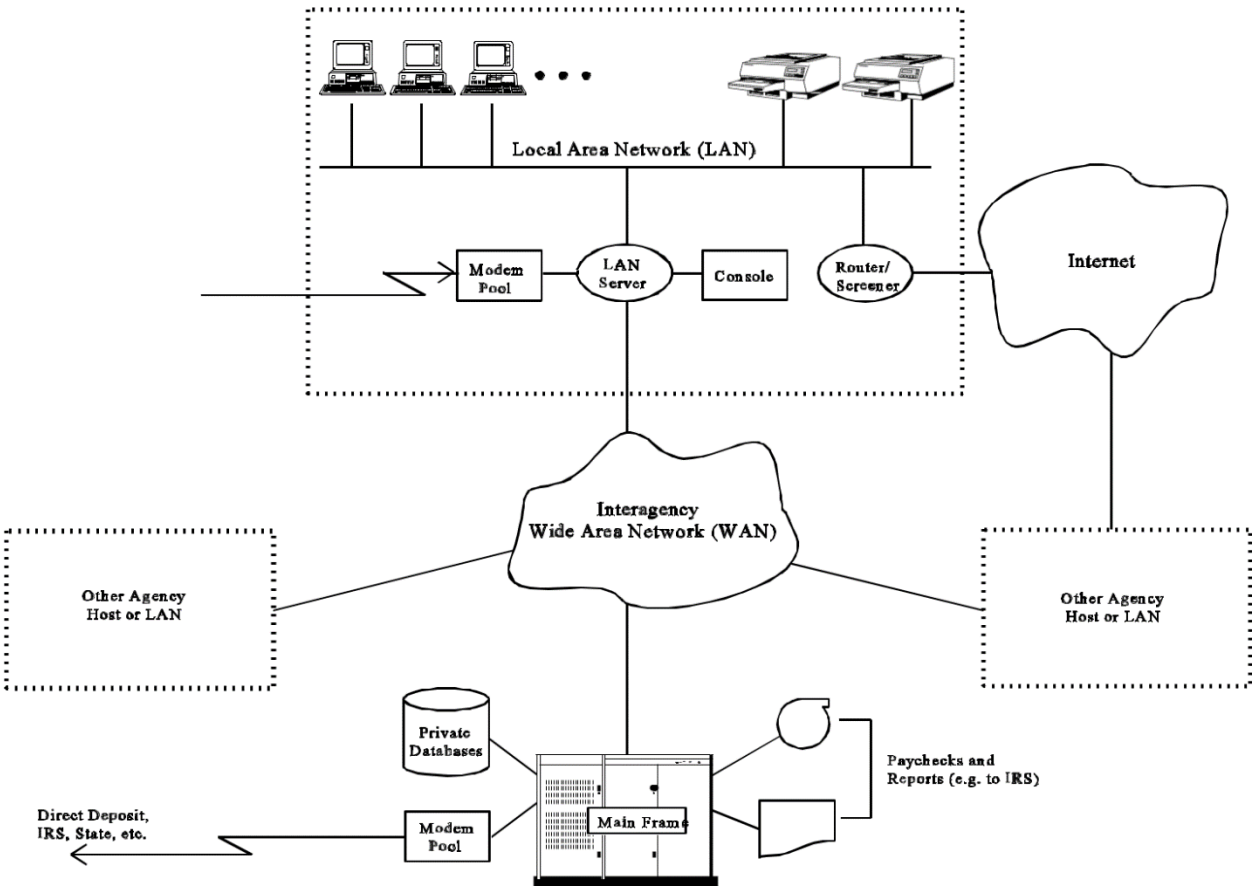
The information system type of HGA is a major application.

9. General System Description / Purpose

HGA's systems play a key role in transferring U.S. Government funds to individuals in the form of paychecks.

10. System Environment

All the PC's in HGA are connected to LAN so that the users can share information among themselves. LAN Server is a central component which also provides a large disk storage for shared information and shared programs. There are several printers distributed throughout the HGA building. LAN provides a connection to the internet via router. A modem pool is provided for dial up connections. A special console is provided for administrative purposes. A WAN is provided so that information can be transferred to or from other agencies.



11.System Interconnections / Information Sharing

System Name: Interagency Wide Network

Organization Type: Telecommunications

Agreement: Government Agency

Date: August 12, 1996

FIPS 199 Category: High

C&A Status: NIST Accredited

Authorizing Official: Sophia C Thompson

System Name: Mainframe

Organization Type: Federal Agency

Agreement: 10-year Contract

Date: May 6, 1990

FIPS 199 Category: High

C&A Status: NIST Accredited

Authorizing Official: Sophia C Thompson

12. Related Laws / Regulations / Policies

There are several Laws, Regulations and Policies that HGA must abide:

- The Computer Fraud and Abuse Act of 1986
- The Computer Security Act of 1997
- Privacy Act
- Gramm–Leach–Bliley
- Sarbanes–Oxley Act
- FIPS-199

13. Minimum Security Controls

Control	Implementation	Status	Control type	Authority responsible
Risk Management(M1)	Risk and security program management themes with risk-driven safeguards	Implemented	Common	CRO
Review of Security Controls(M2)	There are new security controls implemented based on recommendations.	Implemented	Common	CSO
Life Cycle(M3)	System development life cycle implemented	Implemented	Common	CIO
Authorize Processing (M4)	Systems are certified and accredited on regular basis	Implemented	Common	CISO
System Security Plan(M5)	A System Security Plan has been implemented	Implemented	Common	CISO
Personnel Security(O1)	A Security plan for all personnel has been implemented	Implemented	Common	CISO
Physical Security(O2)	Only a few controls for physical security has been implemented	Partially Implemented	Common	CISO
Production, Input/output Controls(O3)	Media and user controls not implemented	Not Implemented	Common	CSO
Contingency Planning(O4)	A comprehensive contingency plan should be developed	Not Implemented	Common	CISO
Hardware and Systems Software Maintenance(O5)	Access controls are limited and have been tested and implemented	Implemented	Common	COG Director
Data Integrity(O6)	Data Integrity checks and tools have to be implemented	Not Implemented	Common	COG Director

Documentation(O7)	Sufficient Documentation has not been provided	Partially Implemented	Common	COG Director
Security Awareness, Training and Education(O8)	Adequate Security training and awareness is provided	Implemented	Common	CISO
Incident Response Capability(O9)	Incident Response Plan is in plan	Implemented	Common	CISO
Identification and Authentication (T1)	Poor Authentication mechanisms are in place.	Partially Implemented	Common	CSO
Logical Access Control (T2)	Sufficient Logical Access control mechanisms are in place	Implemented	Common	CISO
Audit Trails (T3)	Audit logging capabilities are not in place	Not Implemented	Common	CSO

14. Information System Security Plan Completion Date

October 6, 2019

15. Information System Security Plan Approval Date

October 7, 2019

IV. List of Assets with Values

Hypothetical government agency (HGA) has information systems that comprise of different kind of assets which includes financial resources, personnel information, contracting and procurement documents etc. which needs protection. HGA employs 500 personnel. The company has a total of 600 PCs, 50 Printers, 30 modem pools, 10 LAN servers, 20 consoles, and 40 routers. The average cost of each component is as follows:

- PC - $600
- LAN Server - $4000
- Printer - $200
- Model Pool - $200
- Console - $2000
- Router - $400

- **Information Assets inventory**

No.	Asset	Value
A1	Financial Resources	$25,000,000
A2	System Components	$472,000
A21	PC's	$360,000
A22	LAN Server	$40,000
A23	Printers	$10,000
A24	Modem Pool	$6000
A25	Console	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000
A4	Contracting and Procurement Documents	$2,000,000
A5	Draft Regulations	$100,000
A6	Internal Correspondence	$500,000
A7	Business Documents	$2,000,000
A8	Reputation	Intangible
A9	Employee Confidence	Intangible

- **Subset of Assets:**

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000

V. List of Threats

- **List of Threats:**

No.	Threats
T1	Payroll Fraud
T2	Payroll Errors
T3	Interruption of Operations
T4	Disclosure or Brokerage of Information
T5	Network-Related Attacks
T6	Other Threats

- **Selection of subset of threats:**

No.	Threats
T1	Payroll Fraud
T2	Payroll Errors
T4	Disclosure or Brokerage of Information
T5	Network-Related Attacks

VI. List of Vulnerabilities

- **List of Security Vulnerabilities:**

No.	Vulnerabilities
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

- **Selection of subset of vulnerabilities:**

No.	Vulnerabilities
V1.2	Unauthorized Access
V3.4	Accidental Corruption and Loss of Data
V4	Vulnerabilities Related to Disclosure or Brokerage of information
V5	Vulnerabilities Related to Network-Related Attacks

VII. Threat / Vulnerability Pairs

- **List of threat vulnerability pairs:**

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	80%	30%	60%	50%
V3.4 on A1,A22,A26,A3	30%	60%	20%	50%
V4 on A1,A22,A26,A3	20%	10%	80%	30%
V5 on A1,A22,A26,A3	40%	20%	50%	80%

VIII. Assets Impacted by Threat / Vulnerability Pairs

- **List of assets impacted by Threat / vulnerability pairs**

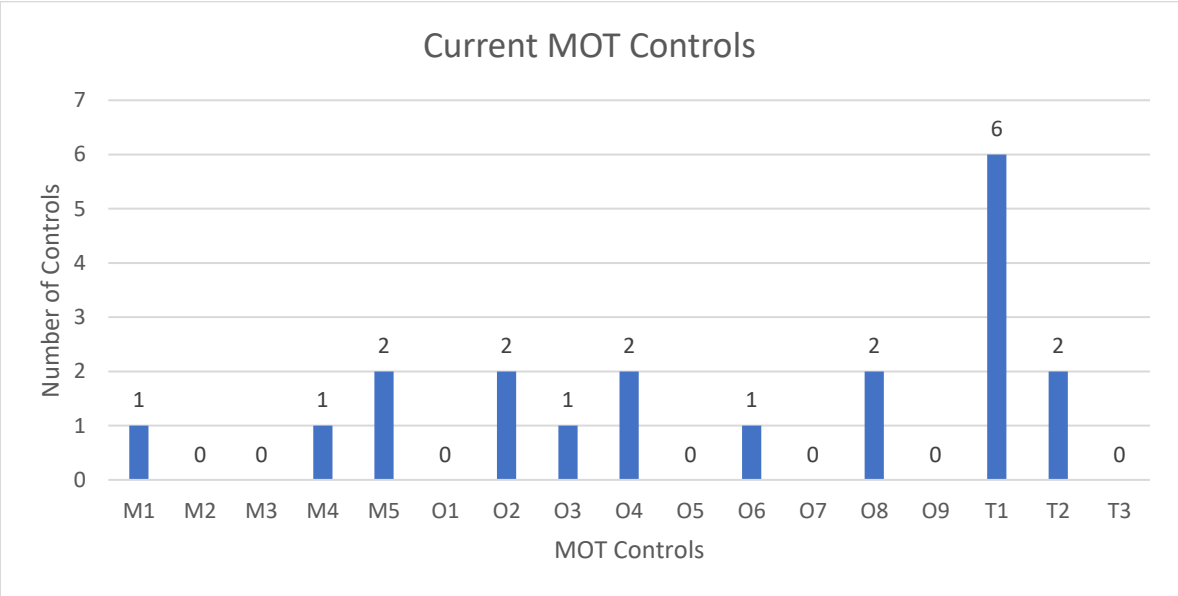
Asset	Vulnerability
A1: Financial Resources	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks
A2: LAN Server	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks

Asset	Vulnerability
A3: Router	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks
A4: Personnel Information	Unauthorized Access
	Accidental Corruption and Loss of Data
	Vulnerabilities Related to Disclosure or Brokerage of information
	Vulnerabilities Related to Network-Related Attacks

IX. MOT – which MOT controls are covered by current HGA controls (Histogram)

Management	Operational	Technical
Risk Management (M1)	Personnel Security (O1)	Identification and Authentication (T1)
Review of Security Controls (M2)	Physical Security (O2)	Logical Access Control (T2)
Life Cycle (M3)	Production, Input/output Controls (O3)	Audit Trails (T3)
Authorize Processing (M4)	Contingency Planning (O4)	
System Security Plan (M5)	Hardware and Systems Software and Maintenance (O5)	
	Data Integrity (O6)	
	Documentation (O7)	
	Security Awareness, Training and Education (O8)	
	Incident Response Capability (O9)	

No.	Security Controls	MOT
C1	General Use and Administrative Controls	
C1.1	Login IDs and Passwords	T1
C1.2	Written Authorization	T1
C1.3	Training and Awareness Session	O8,M5
C1.4	Acknowledgement Forms	T1
C2	Protection Against Payroll Fraud and Errors	
C2.1	Protection Against Unauthorized Execution	T1
C2.2	Protection Against Payroll Errors	T2
C2.3	Protection Against Accidental Corruption or Loss of Payroll Data	O6
C3	Protection Against Interruption of Operations	
C3.1	COG Contingency Planning	O4
C3.2	Division Contingency Planning	O4
C4	Protection Against Disclosure or Brokerage of Information	
C4.1	Secure Storage	O2,O3
C4.2	HGA PC Lock	O2
C4.3	LAN Access Controls	T2
C4.4	Security Awareness Training	O8
C5	Protection Against Network-Related Threats	T1,M1,M5
C6	Protection Against Risks from Non–HGA Computer Systems	T1,M4

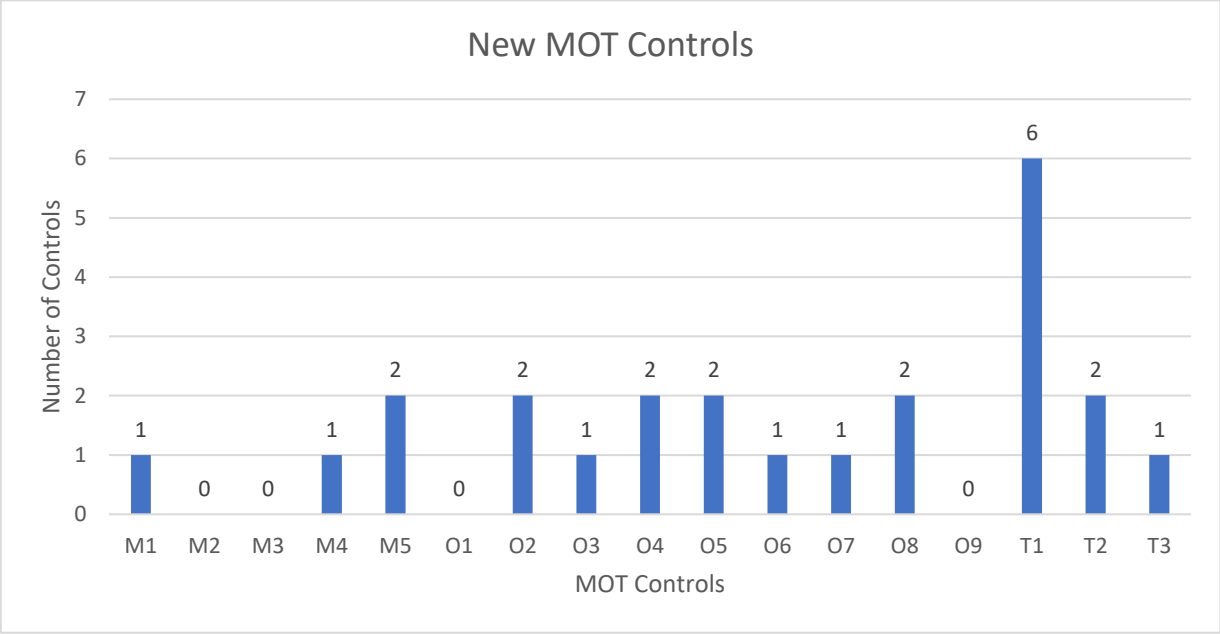


X. MOT – which MOT controls are covered by current AND proposed by new CISO HGA controls AND VPN server AND DMZ (Histogram)

No.	New Controls	MOT
NC1	Controls Mitigating Vulnerabilities Related to Payroll Fraud	
NC1.1	Server Administrative procedures and bug-fixes	O5,O3
NC1.2	One-time passwords	T1
NC1.3	Digital signatures	T1
NC2	Controls Mitigating Payroll Error	T3
NC3	Controls Mitigating Vulnerabilities Related to Continuity of Operations	
NC3.1	SETA	O8
NC3.2	Mainframe MOU	O7,O4
NC3.3	Automated E-mail Reminders and Back-ups	O5,O4
NC4	Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	
NC4.1	Screen locks	T1,O2
NC4.2	Hard Disk Encryption	O2
NC5	Controls Vulnerabilities Related to Network-Related Attacks	
NC5.1	Stronger I&A	T1,,T2,O8
NC5.2	Encrypting modems	M1
NC5.3	Mainframe Communications Encryption	M1,M4

Values for VPN – M5, O6, T1,

Values for DMZ – M5, T2,T1



XI. Security Risk Prevention Strategy 1

Security Risk ($) 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.

List of Information Assets Inventory:

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000

Threat Vulnerability matrix with probability of exploitation

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	40%	8%	30%	20%
V3.4 on A1,A22,A26,A3	10%	40%	80%	30%
V4 on A1,A22,A26,A3	8%	8%	30%	10%
V5 on A1,A22,A26,A3	6%	6%	10%	30%

Initial Risk Impacts:

If a threat exploits a vulnerability, we assume that the risk impact would be 100% or the resilience would be 0%.

	T1*V1.2	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V3.4	T4*V4	T4*V5
A1-100	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A22-85	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A26-90	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A3-95	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Risk Calculations:

- **Risk of A1:**
  $25,000,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $91,500,000> $25,000,000, therefore Risk of A1= $25,000,000 (total asset loss)
- **Risk of A22:**
  $40,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $146,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)
- **Risk of A26:**
  $16,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $58560> $16,000, therefore Risk of A26= $16,000 (total asset loss)
- **Risk of A3:**
  $5,000,000*(40%+8%+30%+20%+10%+40%+80%+30%+8%+8%+30%+10%+6%+6%+10%+30%) = $183,00,000> $5,000,000, therefore Risk of A3= $5,000,000 (total asset loss)

  Thus, residual risk of all assets is $30,056,000.

- **Risk due to V1.2:** $25,000,000*(40%+8%+30%+20%) + $40,000*(40%+8%+30%+20%) + $16,000*(40%+8%+30%+20%) + $5,000,000*(40%+8%+30%+20%) = $29,454,880
- **Risk due to V3.4:** $25,000,000*(10%+40%+80%+30%) + $40,000*(10%+40%+80%+30%) + $16,000*(10%+40%+80%+30%) + $5,000,000*(10%+40%+80%+30%) = $48,089,600
- **Risk due to V4:** $25,000,000*(8%+8%+30%+10%) + $40,000*(8%+8%+30%+10%) + $16,000*(8%+8%+30%+10%) + $5,000,000*(8%+8%+30%+10%) = $16,831,360
- **Risk due to V5:** $25,000,000*(6%+6%+10%+30%) + $40,000*(6%+6%+10%+30%) + $16,000*(6%+6%+10%+30%)+ $5,000,000*(6%+6%+10%+30%) = 15,029,120

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A3: Personnel Information
3	A22: LAN Server
4	A26: Router

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V4: Vulnerabilities Related to Disclosure or Brokerage of information
4	V5: Vulnerabilities Related to Network-Related Attacks

XII. Security Risk Prevention Strategy 2

Security Risk ($) 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.

The highest ranked vulnerability in my case is V3.4: Accidental Corruption and loss of data. Data backups are a good way to safeguard against data loss. As the data is important, it is necessary to store the data at multiple offsite locations.

Updated Threat/Vulnerability pairs with further reduced probabilities:

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	40%	8%	30%	20%
V3.4 on A1,A22,A26,A3	8%	20%	40%	20%
V4 on A1,A22,A26,A3	8%	8%	30%	10%
V5 on A1,A22,A26,A3	6%	6%	10%	30%

Initial Risk Impacts:

If a threat exploits a vulnerability, we assume that the risk impact would be 100% or the resilience would be 0%.

	T1*V1.2	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V3.4	T4*V4	T4*V5
A1-100	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A22-85	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A26-90	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A3-95	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Risk Calculations:

Risk on A1:
100*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 294 > 100, therefore Risk of A1 = 100 (total asset loss)

Risk on A22:

85*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 249.9 > 85, therefore Risk of A22 = 85 (total asset loss)

Risk on A26:

90*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 264.6 > 90, therefore Risk of A26 = 90 (total asset loss)

Risk on A3:

95*(40%+8%+30%+20%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 279.3 > 95, therefore Risk of A3 = 95 (total asset loss)

Thus, Residual risk of all assets is 370.

Risk due to V1.2: 100*(40%+8%+30%+20%) + 85*(40%+8%+30%+20%) + 90*(40%+8%+30%+20%) + 95*(40%+8%+30%+20%) = 362.6

Risk due to V3.4: 100*(8%+20%+40%+20%) + 85*(8%+20%+40%+20%) + 90*(8%+20%+40%+20%) + 95*(8%+20%+40%+20%) = 325.6

Risk due to V4: 100*(8%+8%+30%+10%) + 85*(8%+8%+30%+10%) + 90*(8%+8%+30%+10%) + 95*(8%+8%+30%+10%) = 207.2

Risk due to V5: 100*(6%+6%+10%+30%) + 85*(6%+6%+10%+30%) + 90*(6%+6%+10%+30%) + 95*(6%+6%+10%+30%) = 192.4

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A3: Personnel Information
3	A26: Router
4	A22: LAN Server

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V1.2: Unauthorized Access
2	V3.4: Accidental Corruption and Loss of Data
3	V4: Vulnerabilities Related to Disclosure or Brokerage of information
4	V5: Vulnerabilities Related to Network-Related Attacks

XIII. Security Risk Prevention Strategy 3

Security Risk ($) 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.

Missing M-O-T Controls:

- **Cryptography** (No hard disk encryption)
- **Audit Trails** (No Activity logs)
- **Security considerations**
- **Assurance**

Now, the highest ranked vulnerability risk is V1.2: Unauthorized access. Upgrading to use of one-time passwords for time and attendance sessions on the server. Also, digital signatures on the mainframes based on public key cryptography can be employed to detect unauthorized modification of time and attendance data.

- **Updated Threat/Vulnerability pairs with further reduced probabilities:**

Vulnerabilities/Threats	T1	T2	T3	T4
V1.2 on A1,A22,A26,A3	30%	6%	20%	10%
V3.4 on A1,A22,A26,A3	8%	20%	40%	20%
V4 on A1,A22,A26,A3	8%	8%	30%	10%
V5 on A1,A22,A26,A3	6%	6%	10%	30%

- **Initial Risk Impacts:**

If a threat exploits a vulnerability, we assume that the risk impact would be 100% or the resilience would be 0%.

	T1*V1.2	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V3.4	T4*V4	T4*V5
A1-100	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A22-85	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A26-90	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A3-95	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Risk Calculations:

- **Risk on A1:**
  100*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 262 > 100, therefore Risk of A1 = 100 (total asset loss)
- **Risk on A22:**
- 85*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 222.7 > 85, therefore Risk of A22 = 85 (total asset loss)
- **Risk on A26:**
- 90*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 235.8 > 90, therefore Risk of A26 = 90 (total asset loss)
- **Risk on A3:**
- 95*(30%+6%+20%+10%+8%+20%+40%+20%+8%+8%+30%+10%+6%+6%+10%+30%) = 248.9 > 95, therefore Risk of A3 = 95 (total asset loss)

Thus, Residual risk of all assets is 370.

- **Risk due to V1.2:** 100*(30%+6%+20%+10%) + 85*(30%+6%+20%+10%) + 90*(30%+6%+20%+10%) + 95*(30%+6%+20%+10%) = 244.2
- **Risk due to V3.4:** 100*(8%+20%+40%+20%) + 85*(8%+20%+40%+20%) + 90*(8%+20%+40%+20%) + 95*(8%+20%+40%+20%) = 325.6
- **Risk due to V4:** 100*(8%+8%+30%+10%) + 85*(8%+8%+30%+10%) + 90*(8%+8%+30%+10%) + 95*(8%+8%+30%+10%) = 207.2
- **Risk due to V5:** 100*(6%+6%+10%+30%) + 85*(6%+6%+10%+30%) + 90*(6%+6%+10%+30%) + 95*(6%+6%+10%+30%) = 192.4

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A3: Personnel Information
3	A26: Router
4	A22: LAN Server

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V4: Vulnerabilities Related to Disclosure or Brokerage of information
4	V5: Vulnerabilities Related to Network-Related Attacks

Compare HGA current, CISO proposed, and VPN and DMZ risk controls to the 157 risk controls from Common Criteria

After the initial risk assessment, new controls were proposed by the new CISO's team. The HGA management have successfully implemented most of the controls from the Common Criteria. However, they were a few controls left out like the physical and environmental security controls which are yet to be implemented. Some of the missing MOT controls. VPN and DMZ were implemented to harden the security controls of the HGA. Some of the missing MOT controls are:

- Cryptography (No hard disk encryption)
- Audit Trails (No Activity logs)
- Security considerations
- Assurance

Some of the controls which have been implemented by following the Common Criteria are:

- Cryptography (encryption)
- Media Access Protection

XIV. Security Risk Prevention Strategy and Security Risk Response (Resilience) Strategy

Apply Hardening Controls to highest ranked Residual Asset Risk, thus reducing Risk Impact probabilities, and further reducing the overall security asset residual risk. Calculate residual risks for assets and total HGA residual risk. Provide a ranking for which vulnerability should be addressed by controls first, second, third etc. and a ranking for which risk impact 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.

❖ **Security Risk Prevention Strategy:**

- **Information Assets inventory**

No.	Asset	Value
A1	Financial Resources	$25,000,000
A2	System Components	$472,000
A21	PC's	$360,000
A22	LAN Server	$40,000
A23	Printers	$10,000
A24	Modem Pool	$6000
A25	Console	$40,000
A26	Router	$16,000
A3	Personnel Information	$5,000,000
A4	Contracting and Procurement Documents	$2,000,000
A5	Draft Regulations	$100,000
A6	Internal Correspondence	$500,000
A7	Business Documents	$2,000,000
A8	Reputation	Intangible
A9	Employee Confidence	Intangible

List of Information Assets Inventory:

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A24	VPN Server	$6000
A26	Router	$16,000
A3	DMZ	$50,000
A4	Personnel Information	$5,000,000

Threat Vulnerability Pairs

Vulnerabilities/Threats	T1	T2	T3	T4	T5
V1.2 on A1,A22,A24,A26,A3,A4	40%	8%	30%	20%	10%
V1.4 on A1,A22,A24,A26,A3,A4	20%	10%	30%	10%	20%
V3.4 on A1,A22,A24,A26,A3,A4	10%	40%	80%	30%	10%
V4 on A1,A22,A24,A26,A3,A4	8%	8%	30%	10%	30%
V5 on A1,A22,A24,A26,A3,A4	6%	6%	10%	30%	10%

Calculations:

Risk of A1:
$25,000,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $129,000,000> $25,000,000, therefore Risk of A1= $25,000,000 (total asset loss)

Risk of A22:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A24:

$6000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $30960> $16,000, therefore Risk of A24= $6,000 (total asset loss)

Risk of A26:
$16,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $82560> $16,000, therefore Risk of A26= $16,000 (total asset loss)

Risk of A3:

$50,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,000> $50,000, therefore Risk of A3= $50,000 (total asset loss)

Risk of A4:
$5,000,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,00,000> $5,000,000, therefore Risk of A3= $5,000,000 (total asset loss)

Thus, residual risk of all assets is $30,112,000.

Risk due to V1.2: $25,000,000*(40%+8%+30%+20%+10%) + $40,000*(40%+8%+30%+20%+10%) + $6,000*(40%+8%+30%+20%+10%) + $16,000*(40%+8%+30%+20%+10%) + $50,000*(40%+8%+30%+20%+10%) + $5,000,000*(40%+8%+30%+20%+10%) = $32,520,960

Risk due to V1.4: $25,000,000*(20%+10%+30%+10%+20%) + $40,000*(20%+10%+30%+10%+20%) + $6,000*(20%+10%+30%+10%+20%) + $16,000*(20%+10%+30%+10%+20%) + $50,000*(20%+10%+30%+10%+20%) + $5,000,000*(20%+10%+30%+10%+20%) = $27,100,800

Risk due to V3.4: $25,000,000*(10%+40%+80%+30%+10%) + $40,000*(10%+40%+80%+30%+10%) + $6,000*(10%+40%+80%+30%+10%) + $16,000*(10%+40%+80%+30%+10%) + $50,000*(10%+40%+80%+30%+10%) + $5,000,000*(10%+40%+80%+30%+10%) = $51,190,400

Risk due to V4: $25,000,000*(8%+8%+30%+10%+30%) + $40,000*(8%+8%+30%+10%+30%) + $6,000*(8%+8%+30%+10%+30%) + $16,000*(8%+8%+30%+10%+30%) + $50,000*(8%+8%+30%+10%+30%) + $5,000,000*(8%+8%+30%+10%+30%) = $25,896,320

Risk due to V5: $25,000,000*(6%+6%+10%+30%+10%) + $40,000*(6%+6%+10%+30%+10%) +$6,000*(6%+6%+10%+30%+10%) + $16,000*(6%+6%+10%+30%+10%) + $50,000*(6%+6%+10%+30%+10%) + $5,000,000*(6%+6%+10%+30%+10%) = 18,669,440

Ranking of security asset residual risks:

Rank	Asset
1	A1: Financial Resources
2	A4: Personnel Information
3	A3: DMZ
4	A22: LAN Server
5	A26: Router
6	A24: VPN Server

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V1.4: Unauthorized Modification of time and Attendance sheets
4	V4: Vulnerabilities Related to Disclosure or Brokerage of information
5	V5: Vulnerabilities Related to Network-Related Attacks

❖ **Security Risk Response Strategy:**

No.	Assets	Asset value
A1	Financial Resources	$25,000,000
A22	LAN Server	$40,000
A24	VPN Server	$6000
A25	Console	$40,000
A26	Router	$16,000
A3	DMZ	$50,000
A4	Personnel Information	$5,000,000

Threat/Vulnerability pairs with further reduced probabilities:

Vulnerabilities/Threats	T1	T2	T3	T4	T5
V1.2 on A1,A22,A24,A26,A3,A4	40%	8%	30%	20%	10%
V1.4 on A1,A22,A24,A26,A3,A4	20%	10%	30%	10%	20%
V3.4 on A1,A22,A24,A26,A3,A4	10%	40%	80%	30%	10%
V4 on A1,A22,A24,A26,A3,A4	8%	8%	30%	10%	30%
V5 on A1,A22,A24,A26,A3,A4	6%	6%	10%	30%	10%

The highest ranked Residual Asset Risk is the A1: Financial Resources. We now apply hardening controls to reduce the residual risk of financial resources.

	T1*V1.2	T1*V1.4	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V1.4	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V1.4	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V1.4	T4*V3.4	T4*V4	T4*V5	T5*V1.2	T5*V1.4	T5*V3.4	T5*V4	T5*V5
A1	80%	60%	70%	90%	60%	90%	70%	60%	80%	70%	90%	80%	60%	70%	80%	60%	70%	90%	80%	70%	60%	90%	80%	70%	60%
A22	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%
A24	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%
A25	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%
A26	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%
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%
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%

Risk Calculations:

Risk of A1:
25,000,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%+20%*60%+10%*70%+30%*80%+10%*70%+20%*90%+10%*70%+40%*60%+80%*60%+30%*90%+10%*80%+8%*90%+8%*80%+30%*70%+10%*80%+30%*70%+6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = $15,165,000<$25,000,000, therefore Risk of A1 = $15,165,000 (partial asset loss)

Risk of A22:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A24:

$6000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $30,960> $6,000, therefore Risk of A24= $6,000 (total asset loss)

Risk of A25:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A26:
$16,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $82,560> $16,000, therefore Risk of A26= $16,000 (total asset loss)

Risk of A3:

$50,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,000> $50,000, therefore Risk of A3= $50,000 (total asset loss)

Risk of A4:
$5,000,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $25,800,000> $5,000,000, therefore Risk of A3= $5,000,000 (total asset loss)

Thus, residual risk of all assets is $20,317,000.

Risk due to V1.2: $25,000,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%) + $40,000*(40%+8%+30%+20%+10%) + $6,000*(40%+8%+30%+20%+10%) + $40,000*(40%+8%+30%+20%+10%) $16,000*(40%+8%+30%+20%+10%) + $50,000*(40%+8%+30%+20%+10%) + $5,000,000*(40%+8%+30%+20%+10%) = $32,520,960

Risk due to V1.4: $25,000,000*(20%*60%+10%*70%+30%*80%+10%*70%+20%*90%) + $40,000*(20%+10%+30%+10%+20%) + $6,000*(20%+10%+30%+10%+20%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(20%+10%+30%+10%+20%) + $50,000*(20%+10%+30%+10%+20%) + $5,000,000*(20%+10%+30%+10%+20%) = $21,636,800

Risk due to V3.4: $25,000,000*(10%*70%+40%*60%+80%*60%+30%*90%+10%*80%) + $40,000*(10%+40%+80%+30%+10%) + $6,000*(10%+40%+80%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(10%+40%+80%+30%+10%) + $50,000*(10%+40%+80%+30%+10%) + $5,000,000*(10%+40%+80%+30%+10%) = $37,258,400

Risk due to V4: $25,000,000*(8%*90%+8%*80%+30%*70%+10%*80%+30%*70%) + $40,000*(8%+8%+30%+10%+30%) + $6,000*(8%+8%+30%+10%+30%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(8%+8%+30%+10%+30%) + $50,000*(8%+8%+30%+10%+30%) + $5,000,000*(8%+8%+30%+10%+30%) = $20,330,720

Risk due to V5: $25,000,000*(6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) + $40,000*(6%+6%+10%+30%+10%) +$6,000*(6%+6%+10%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(6%+6%+10%+30%+10%) + $50,000*(6%+6%+10%+30%+10%) + $5,000,000*(6%+6%+10%+30%+10%) = 13,894,240

Ranking of security asset residual risks: Ranking of security asset residual risks:

Rank	Asset	Value
1	A4: Personnel Information	$5,000,000
2	A1: Financial Resources	$15,165,000
3	A3: DMZ	$50,000
4	A22: LAN Server	$40,000
5	A25: Console	$40,000
6	A26: Router	$16,000
7	A24: VPN Server	$6000

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V1.4: Unauthorized Modification of time and Attendance sheets
4	V4: Vulnerabilities Related to Disclosure or Brokerage of information
5	V5: Vulnerabilities Related to Network-Related Attacks

- **Mixed Strategy:**

The highest ranked Residual Asset now is the A4: Personnel Information. We now apply hardening controls to reduce the residual risk of this asset.

Threat/Vulnerability pairs with further reduced probabilities:

Vulnerabilities/Threats	T1	T2	T3	T4	T5
V1.2 on A1,A22,A24,A26,A3,A4	40%	8%	30%	20%	10%
V1.4 on A1,A22,A24,A26,A3,A4	20%	10%	30%	10%	20%
V3.4 on A1,A22,A24,A26,A3,A4	10%	40%	80%	30%	10%
V4 on A1,A22,A24,A26,A3,A4	8%	8%	30%	10%	30%
V5 on A1,A22,A24,A26,A3,A4	6%	6%	10%	30%	10%

Risk Matrix:

	T1*V1.2	T1*V1.4	T1*V3.4	T1*V4	T1*V5	T2*V1.2	T2*V1.4	T2*V3.4	T2*V4	T2*V5	T3*V1.2	T3*V1.4	T3*V3.4	T3*V4	T3*V5	T4*V1.2	T4*V1.4	T4*V3.4	T4*V4	T4*V5	T5*V1.2	T5*V1.4	T5*V3.4	T5*V4	T5*V5
A1	80%	60%	70%	90%	60%	90%	70%	60%	80%	70%	90%	80%	60%	70%	80%	60%	70%	90%	80%	70%	60%	90%	80%	70%	60%
A22	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%
A24	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%
A25	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%
A26	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%
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%
A4	80%	60%	70%	90%	60%	90%	70%	60%	80%	70%	90%	80%	60%	70%	80%	60%	70%	90%	80%	70%	60%	90%	80%	70%	60%

Risk Calculations:

Risk of A1:
15,165,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%+20%*60%+10%*70%+30%*80%+10%*70%+20%*90%+10%+70%+40%*60%+80%*60%+30%*90%+10%+80%+8%*90%+8%*80%+30%*70%+10%*80%+30%+70%+6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = 9,199,089<15,165,000, therefore Risk of A1 = $9,199,089 (partial asset loss)

Risk of A22:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A24:

$6000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $30,960> $6,000, therefore Risk of A24= $6,000 (total asset loss)

Risk of A25:
$40,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $206,400> $40,000, therefore Risk of A22= $40,000 (total asset loss)

Risk of A26:
$16,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $82,560> $16,000, therefore Risk of A26= $16,000 (total asset loss)

Risk of A3:

$50,000*(40%+8%+30%+20%+10%+20%+10%+30%+10%+20%+10%+40%+80%+30%+10%+8%+8%+30%+10%+30%+6%+6%+10%+30%+10%) = $258,000> $50,000, therefore Risk of A3= $50,000 (total asset loss)

Risk of A4:
$5,000,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%+20%*60%+10%*70%+30%*80%+10%*70%+20%*90%+10%+70%+40%*60%+80%*60%+30%*90%+10%+80%+8%*90%+8%*80%+30%*70%+10%*80%+30%+70%+6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = $3,033,000< $5,000,000, therefore Risk of A3= $3,033,000 (partial asset loss)

Thus, residual risk of all assets is $12,384,089

Risk due to V1.2: $15,165,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%) + $40,000*(40%+8%+30%+20%+10%) + $6,000*(40%+8%+30%+20%+10%) + $40,000*(40%+8%+30%+20%+10%) $16,000*(40%+8%+30%+20%+10%) + $50,000*(40%+8%+30%+20%+10%) + $3,033,000*(40%*80%+8%*90%+30%*90%+20%*60%+10%*60%) = $15,486,876

Risk due to V1.4: $15,165,000*(20%*60%+10%*70%+30%*80%+10%*70%+20%*90%) + $40,000*(20%+10%+30%+10%+20%) + $6,000*(20%+10%+30%+10%+20%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(20%+10%+30%+10%+20%) + $50,000*(20%+10%+30%+10%+20%) + $3,033,000*(20%*60%+10%*70%+30%*80%+10%*70%+20%*90%) = $12,511,440

Risk due to V3.4: $15,165,000*(10%*70%+40%*60%+80%*60%+30%*90%+10%*80%) + $40,000*(10%+40%+80%+30%+10%) + $6,000*(10%+40%+80%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(10%+40%+80%+30%+10%) + $50,000*(10%+40%+80%+30%+10%) + $3,033,000*(10%*70%+40%*60%+80%*60%+30%*90%+10%*80%) = $21,004,120

Risk due to V4: $15,165,000*(8%*90%+8%*80%+30%*70%+10%*80%+30%*70%) + $40,000*(8%+8%+30%+10%+30%) + $6,000*(8%+8%+30%+10%+30%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(8%+8%+30%+10%+30%) + $50,000*(8%+8%+30%+10%+30%) + $3,033,000*(8%*90%+8%*80%+30%*70%+10%*80%+30%*70%) = $11,704,648

Risk due to V5: $15,165,000*(6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) + $40,000*(6%+6%+10%+30%+10%) +$6,000*(6%+6%+10%+30%+10%) + $40,000*(20%+10%+30%+10%+20%) +$16,000*(6%+6%+10%+30%+10%) + $50,000*(6%+6%+10%+30%+10%) + $3,033,000*(6%*60%+6%*70%+10%*80%+30%*70%+10%*60%) = $7,882,984

Ranking of security asset residual risks: Ranking of security asset residual risks:

Rank	Asset	Value
1	A1: Financial Resources	$15,165,000
2	A4: Personnel Information	$9,199,089
3	A3: DMZ	$50,000
4	A22: LAN Server	$40,000
5	A25: Console	$40,000
6	A26: Router	$16,000
7	A24: VPN Server	$6000

Ranking of vulnerability security risks:

Rank	Vulnerability
1	V3.4: Accidental Corruption and Loss of Data
2	V1.2: Unauthorized Access
3	V1.4: Unauthorized Modification of time and Attendance sheets
4	V4: Vulnerabilities Related to Disclosure or Brokerage of information
5	V5: Vulnerabilities Related to Network-Related Attacks

XV. Conclusion:

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

No, HGA did not address all the security risks based on risk assessment. However, most of the crucial security risks have been addressed.

What would the budget for proposed controls be including controls proposed by new CISO controls and missing MOT controls and VPN and DMZ?

Controls	Estimated Budget
Controls Mitigating Vulnerabilities Related to Payroll Fraud	$100,000
Controls Mitigating Payroll Error	$75,000
Controls Mitigating Vulnerabilities Related to Continuity of Operations	$500,000
Controls Mitigating Vulnerabilities Related to Disclosure or Brokerage of information	$250,000
Controls Vulnerabilities Related to Network-Related Attacks	$200,000
Review of Security Controls	$50,000
Personnel Security	$300,000
VPN	$6000
DMZ	$50,000
Total	$1,531,000

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

HGA has information systems which consists of sensitive information like financial resources, personnel information and intangible assets like reputation and employee confidence. Hence, it a Risk-Averse organization. Being a Risk-Averse organization, I recommend that the company employs a Risk prevention strategy.

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

Residual Risk Reduction = Residual risk with current controls – Residual risk with current controls, new controls, missing MOT controls, VPN and DMZ (mixed strategy)

= $30,056,000 - $12,384,089

= $17,671,911

Thus, residual risk reduction exceeds the budget for proposed controls.

What is the ((proposed security risk budget Cost) / (expected security risk Benefit)) ratio?

Cost Benefit ratio = (proposed security risk budget cost) / (expected security risk benefit)

= $1,531,000 / $17,671,911

= 0.0866