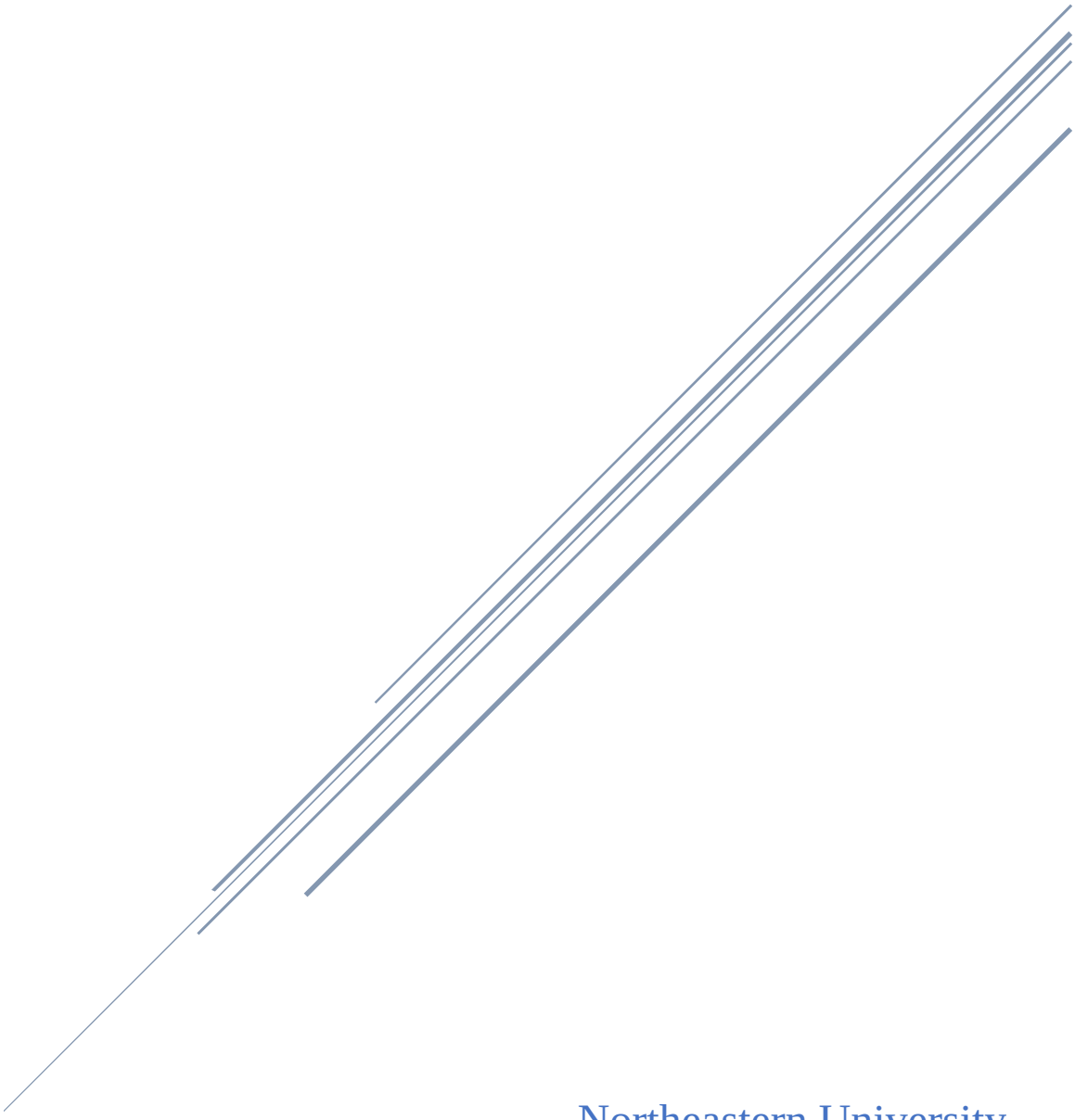
CY5200 SECURITY RISK MANAGEMENT AND ASSESSMENT

Instructor: Professor Themis A. Papageorge



Northeastern University
By Vanessa Kibaja

Table of Contents

PART A: Security Risk Management Assessment ***5***

Executive Summary **6**

List of Assets with Values ($) **8**

Assets Subsets: 8

List of Threats **8**

Threats Subsets: 9

List of Vulnerabilities **9**

Vulnerability Subsets: 9

Threats- Vulnerability Pairs with assigned Likelihood probabilities **10**

Asset- Vulnerability Pairs **10**

MOT controls that are covered by current HGA controls (Histogram) **10**

Current Security Controls and Policies with MOT Controls **11**

MOT controls that are covered by current HGA controls (Histogram) **12**

MOT controls that are covered by current and proposed by new CISO, HGA controls, and VPN server and DMZ (Histogram) **12**

New Security Controls and Policies by the CISO with MOT Controls: **13**

MOT controls that are covered by current and proposed by new CISO, HGA controls, and VPN server and DMZ (Histogram) **14**

Security Risk Prevention Strategy **15**

Assets Subsets: 15

Vulnerability Subsets: 15

Threat/Vulnerability Pairs along with *Reduced* likelihood probabilities in percentage: 15

Initial Risk Impacts (100%, thus 0% Resilience for the worst-case scenario) 15

Calculate Residual Asset Security Risks and Vulnerability Security Risks: 16

Security Risk Prevention Strategy I **17**

List of missing MOT controls: 17

Information assets inventory with values 17

New Vulnerability due to VPN: 18

Threat/Vulnerability Pairs along with *Reduced* likelihood probabilities in percentage: 18

Calculating Residual Asset Security Risks and Vulnerability Security Risks: 19

Security Risk Prevention Strategy Step P2: **21**

Threat/Vulnerability pairs along with *Reduced* likelihood probabilities in percentage: 21

Calculating Residual Asset Security Risks and Vulnerability Security Risks: 21

Security Risk Prevention Strategy Step P3: **23**

Threat/Vulnerability pairs along with *Reduced* likelihood probabilities in percentage: 23

Calculating Residual Asset Security Risks and Vulnerability Security Risks: 23

Security Risk Response (Resilience) Strategy Step R1: **25**

Threat/Vulnerability pairs along from step P3: 25

Calculating Residual Asset Security Risks and Vulnerability Security Risks: 26

Security Risk Response (Resilience) Strategy Step R2: 28
Threat/Vulnerability pairs along from step P3: 28
Updated Risk Impacts 28
Calculating Residual Asset Security Risks and Vulnerability Security Risks: 29
Security Risk Response (Resilience) Strategy Step R3: 31
Calculating Residual Asset Security Risks and Vulnerability Security Risks: 32

Mixed Security Risk Prevention Strategy and Security Risk Response Strategy 35
Threat/Vulnerability pairs along from step P3: 35
Updated Risk Impacts 35
Calculating Residual Asset Security Risks and Vulnerability Security Risks: 36

Conclusion: Cost Benefit Analysis 38
Did the HGA team address all security risks based on your risk assessment for HGA? 38
Do you recommend a Risk Prevention Strategy, a Risk Response Strategy, or a mixed strategy as combination of both? 39
Does the Residual Risk Reduction exceed the budget for proposed controls? 39

PART B: Security Risk Management Implementation Plan 41

1. Access Control Security Risk Management Implementation Controls and Policies 42
List of critical assets 42
List of missing Cybersecurity Implementation Controls 42
List of Potential Vulnerabilities: 42
List of Potential Threats: 43
List of potential Risk 43

2. Network Infrastructure Security Risk Management Implementation Controls and Policies 43
List of critical assets 43
List of missing Cybersecurity Implementation Controls 43
List of Potential Vulnerabilities: 44
List of Potential Threats: 44
List of potential Risk 44

3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies 44
List of critical assets 44
List of missing Cybersecurity Implementation Controls 45
List of Potential Vulnerabilities: 45
List of Potential Threats: 45
List of potential Risk 45

4. Database Security Risk Management Implementation Controls and Policies 45
List of critical assets 46
List of missing Cybersecurity Implementation Controls 46
List of Potential Vulnerabilities: 47
List of Potential Threats: 47
List of potential Risk 47

5. Applications Development Security Risk Management Implementation Controls and Policies 47
List of critical assets 47
List of missing Cybersecurity Implementation Controls 48
List of Potential Vulnerabilities: 48
List of Potential Threats: 48
List of potential Risk 48

5. Wireless Security Risk Management Implementation Controls and Policies 49
List of critical assets 49
List of missing Cybersecurity Implementation Controls 49
List of Potential Vulnerabilities: 49
List of Potential Threats: 50
List of potential Risk 50

List of Cybersecurity Implementation Controls that exist at GrubHub 50
Access Control Security Risk Management Implementation Controls and Policies 50
Network Infrastructure Security Risk Management Implementation Controls and Policies 51
Network Infrastructure Management Security Risk Management Implementation Controls and Policies 52
Database Security Risk Management Implementation Controls and Policies 52
Applications Development Security Risk Management Implementation Controls and Policies 55
Wireless Security Risk Management Implementation Controls and Policies 56

Comparison of the Implementation Controls discussed in class with GrubHub's existing Cybersecurity Implementation Controls 57
Access Control Security Risk Management Implementation Controls and Policies 57
Network Infrastructure Security Risk Management Implementation Controls and Policies 58
Network Infrastructure Management Security Risk Management Implementation Controls and Policies 59
Database Security Risk Management Implementation Controls and Policies 60
Applications Development Security Risk Management Implementation Controls and Policies 62
Wireless Security Risk Management Implementation Controls and Policies 63

List of critical assets that exist at GrubHub 64

List of potential vulnerabilities for critical assets where cybersecurity Implementation Controls are missing 64

List of potential threats to GrubHub that could exploit vulnerabilities of critical assets 65

List of potential risks for critical assets where cybersecurity Implementation Controls are missing. 65

List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks – Risk Prevention Strategy 66

List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience – Risk Response Strategy 67

Ranking of asset risk and Vulnerability risk for GrubHub access control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless. 68
Top 5 Potential Vulnerabilities: 69
Top 5 Potential Risks: 69

List of recommended Hardening Prevention controls and policies for each recommended control that should be created to reduce vulnerability probabilities and thus mitigate the identified risks – Risk Prevention Strategy 69

List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience – Risk Response Strategy 70

Cybersecurity Workforce Risk Management Implementation: 71
List of Cybersecurity Specialty Areas that exist at GrubHub 71

List of Cybersecurity Work Roles that exist at GrubHub 71
List of Cybersecurity Tasks that exist at GrubHub 71

Comparison of the NCWF recommended Cybersecurity Specialty Areas with GrubHub existing Cybersecurity Specialty Areas 75

Comparison of the NCWF recommended Cybersecurity Work Roles and their NCWF recommended Cybersecurity Tasks with GrubHub existing Cybersecurity Work Roles and their existing Cybersecurity Tasks 76

List of potential threats to GrubHub that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, cybersecurity work roles, and cybersecurity tasks. 129
List of potential threats to GrubHub that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, cybersecurity work roles, and cybersecurity tasks. 129
List of recommended policies for each recommended cybersecurity specialty areas, cybersecurity work roles, and cybersecurity tasks that should be created to mitigate the identified risks. 129

PART C: Security Risk Management Recommendations 130

List of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits based on risk management analysis 131

For HGA: 131
For GrubHub: 131
For HGA: 131
For GrubHub: 132

Comparing proposed security controls, methods, and policies budget for HGA with the proposed security controls, methods, and policies budget for GrubHub. 133

Attack Trees 134

For HGA: 134
For GrubHub: 135

Vulnerabilities and Exploitation Probabilities: 136

For HGA: 136
For GrubHub: 136

Cybersecurity workforce recommendations 137

For HGA: 137
For GrubHub: 137

Appendix: 138

Works Cited 140

PART A: Security Risk Management Assessment

Executive Summary

Information System Name: Hypothetical Government Agency (HGA)

Information System Categorization:

Assets	**Impact**		
	Confidentiality	**Integrity**	**Availability**
Financial Resources	High	High	High
System components	High	High	High
Personnel Information	High	High	High
Contracting Documents	High	High	High
Procurement Documents	High	High	High
Draft Regulations	High	High	High
Internal Correspondence	High	High	High
Business Documents	High	High	High
Time and Attendance Records	High	High	High

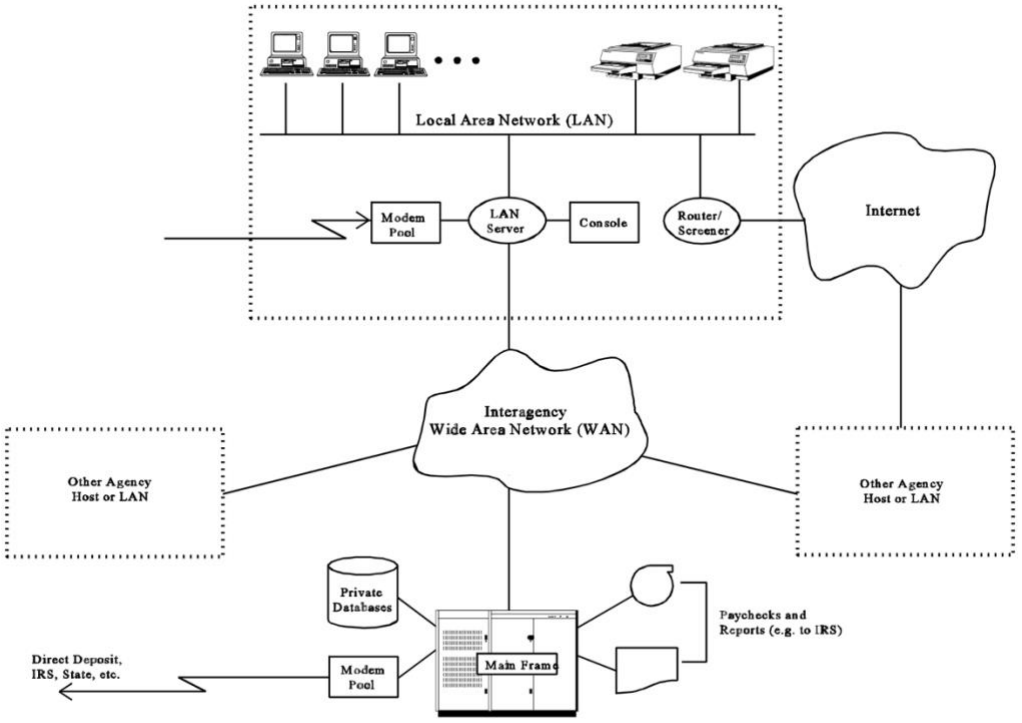
Information System Owner: Name: Vanessa Kibaja Title: Chief Executive Officer (CEO) Agency: Hypothetical Government Agency (HGA) Address: 100 Cambridge Pl, Cambridge, MA, 02140 Email: vkibaja@hga.us Phone: 617-724-1234	**Authorizing Official:** Name: Kenneth James Title: Chief Information Officer (CIO) Agency: Hypothetical Government Agency (HGA) Address: 200 Cambridge Pl, Cambridge, MA, 02140 Email: vkibaja@hga.us Phone: 617-724-9876
Other Designated Contact: Name: Karen Kayombo Title: Chief Financial Officer (CFO) Agency: Hypothetical Government Agency (HGA) Address: 300 Cambridge Pl, Cambridge, MA, 02140 Email: vkibaja@hga.us Phone: 617-724-4321	**Assignment of Security Responsibility:** Name: Novatus Muliro Title: Chief Information Security Officer (CISO) Agency: Hypothetical Government Agency (HGA) Address: 400 Cambridge Pl, Cambridge, MA, 02140 Email: vkibaja@hga.us Phone: 617-724-4567

Information System Operational Status: Operational

Information System Type: Major Application

General System Purpose: HGA transfers U.S Government funds to individuals in Paycheck form.

System Environment:



The image above represents the system architecture of HGA prior to Security Assessment. Systems are connected via LAN, with a modem pool and router for wireless connections. At HGA, we have a Main Frame that handles several tasks such as transferring payments to our customers. The Main Frame is very secured, and it connects to the private database that stores sensitive information. HGA is also connected to other organizations via WAN.

System Interconnections and/or Information Sharing:
System Name: Government Agency
Organization Type: Public Sector Telecommunication Agency
Agreement: Government
Date: July 3rd, 1993
FIPS 199 Category: High
C&A Status: Certified and Accredited
Authorizing Official: Andrew Gasper

Information Security Plan Complete Date: November 18, 2021

Information Security Plan Approval Date: November 20, 2021

List of Assets with Values ($)

Assets Representation	Assets Description	Asset Value
A1	Financial resources	$500000
A2:	***System components***	
A2.1	PCs	$1500000
A2.2	Printers	$1800
A2.3	Routers	$5250
A2.4	Modem Pool	$3000
A2.5	LAN server	$35000
A2.6	Console	$5000
A3	Personal Information	$300000
A4	Contracting & procurement document	$10000
A5	Draft regulations	$10000
A6	Business reports	$10000
A7:	***Intangible assets***	
A7.1	Reputation of agency	Intangible
A7.2	Employee's confidence	Intangible

Assets Subsets:

Asset Representation	Asset Description	Asset Value
A1	Financial Resources	$500000
A3	Personal Information	$300000
A2.3	Routers	$5250
A2.5	LAN Servers	$35000

List of Threats

Threats Representation	Threat Description
T1	Disclosure of sensitive information
T2	Network Threats
T3	Payroll Frauds
T4	Interruption of Operation
T5	Natural Disaster
T6	Payroll errors
T7	Misuse of information
T8	Theft

Threats Subsets:

Threats Representation	Threat Description
T1	Disclosure of sensitive information
T2	Network Threats
T3	Payroll Frauds
T4	Interruption of Operation

List of Vulnerabilities

Vulnerabilities Representation	Vulnerabilities Description
Related to Information Disclosure	
V1	HGA's lack of compliance
V2	Unencrypted data transmission to/from server
V3	Master database stored in mainframe prone to attack
Related to Payroll Fraud	
V4	Falsified Time Sheets
V5	Unauthorized Access
V6	Bogus Time and Attendance Applications
V7	Unauthorized Modification of Time and Attendance Data
Related to Payroll Errors	
V8	COG Contingency Planning
V9	Division Contingency Planning
V10	Virus Prevention
V11	Accidental Corruption and Loss of Data
Related to Network Threats	
V12	Email Copy
V13	Eavesdropping of information during a dial-up interaction

Vulnerability Subsets:

Vulnerability Representation	Vulnerability Description
V2	Unencrypted data transmission to/from server
V3	Master database stored in mainframe prone to attack
V5	Unauthorized Access
V11	Accidental Corruption and Loss of Data

Threats- Vulnerability Pairs with assigned Likelihood probabilities

	T1	**T2**	**T4**	**T8**
V2 on A1, A3, A2.3, & A2.5	94	90	84	94
V3 on A1, A3, A2.3, & A2.5	95	94	92	92
V5 on A1, A3, A2.3, & A2.5	95	90	92	95
V11 on A1, A3, A2.3, & A2.5	94	92	94	95

Asset- Vulnerability Pairs

Assets	**Corresponding vulnerabilities**
A1: Financial Resources	V3: Master database stored in mainframe prone to attack
	V5: Unauthorized Access
	V11: Accidental Corruption and Loss of Data
A3: Personal Information	V2: Unencrypted data transmission to/from server
	V3: Master database stored in mainframe prone to attack
	V5: Unauthorized Access
	V11: Accidental Corruption and Loss of Data
A2.3: Routers	V2: Unencrypted data transmission to/from server
	V5: Unauthorized Access

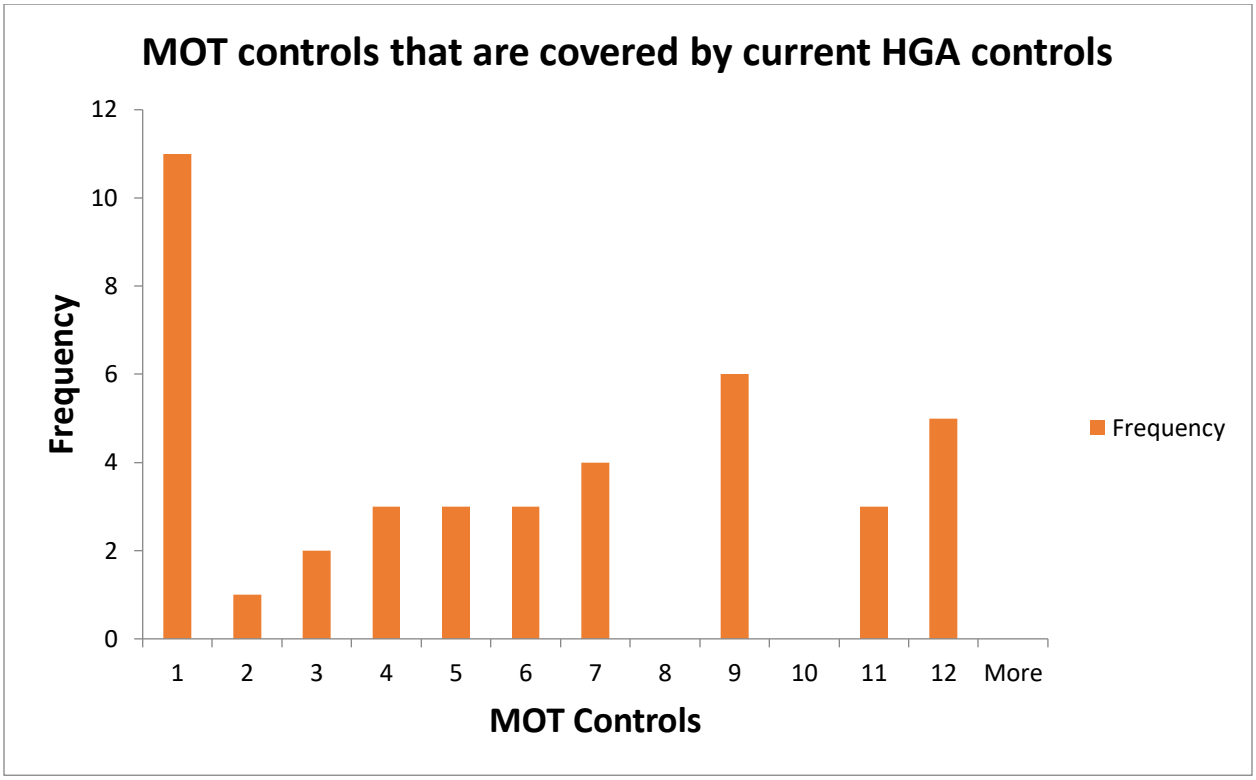
MOT controls that are covered by current HGA controls (Histogram)

Management	**Operational**	**Technical**
MT1- Risk Management	MT5 - Physical security	MT9 - IAM – Identity Authentication
MT2 - Life cycle	MT6 - Contingency planning	MT10 - Audit Trails
MT3 - Security Plan	MT7 - Data Integrity	MT11 -Logical Access Control
MT4- Review of security controls	MT8 - Incident response plan	
	MT12 – Security trainings	

Current Security Controls and Policies with MOT Controls

Security Control Representation	**Security Control Description**	**MOT Controls**
Protection Against Payroll Fraud and Errors on Time and Attendance Application		
SC1	Protect against Unauthorized execution – assign access control	11, 9, 1
SC2	Abide to privacy Act to secure Personal Information	6, 3, 4, 1
SC3	The use of Authentication mechanisms	
SC4	Protection on data loss or corruption	1, 2, 3,
SC5	Protect against Payroll errors - clerks and supervisors review timesheets	6, 9, 4
Protection Against Interruption of Operations		
SC6	COG and Division Contingency Planning	6, 1
Protection Against Computer Systems		
SC7	Employee compliance trainings	12, 1
SC8	Employee awareness on different security policies and controls	12, 1
SC9	The use of unique employee IDs and sign-in credentials	9, 7, 1
Protection Against Information Disclosure		
SC10	Securely storing of Time and Attendance documentation	12, 1
SC11	Keylocks that disables PCs	5,7,1,9, 12
SC12	Access control on Server	11, 9, 7, 5, 1
Protection Against Network Related Threats		
SC13	Access control	9,11,7,5,4,1, 12

MOT controls that are covered by current HGA controls (Histogram)



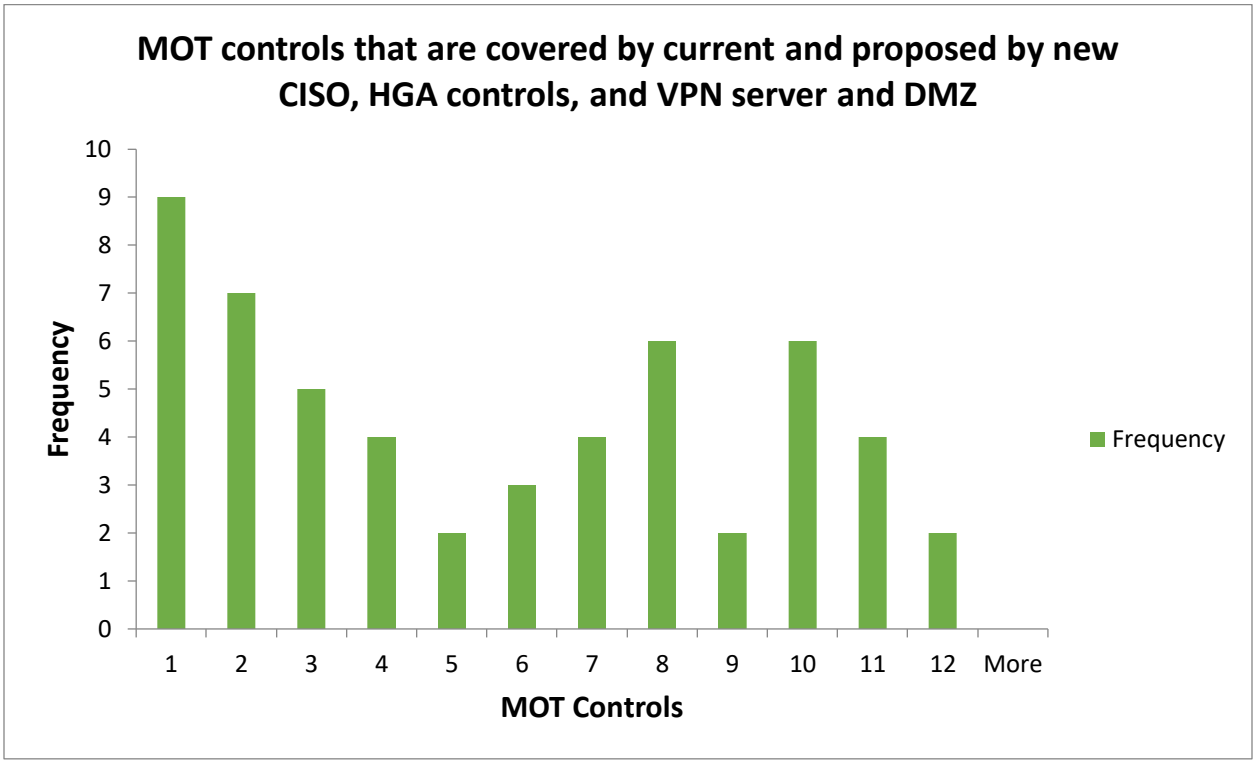
MOT controls that are covered by current and proposed by new CISO, HGA controls, and VPN server and DMZ (Histogram)

Management	**Operational**	**Technical**
MT1- Risk Management	MT5 - Physical security	MT9 - IAM – Identity Authentication
MT2 - Life cycle	MT6 - Contingency planning	MT10 - Audit Trails
MT3 - Security Plan	MT7 - Data Integrity	MT11 -Logical Access Control
MT4- Review of security controls	MT8 - Incident response plan	
	MT12 – Security trainings	

New Security Controls and Policies by the CISO with MOT Controls:

New Security Control Representation	**New Security Control Description**	**MOT Controls**
Security Control Related to Payroll Fraud Vulnerabilities		
NSC1	Digital signatures	9, 1
NSC2	Bug fixes	2, 3, 1
Security Control Related to Payroll Error Vulnerabilities		
NSC3	Establish incentives and penalties for complying with safeguards	1, 2,
Security Control Related to Continuity of Operations Vulnerabilities		
NSC4	COG enforced training on people responsible for contingency planning	12, 1, 3
Security Control Related to Information Disclosure Vulnerabilities		
NSC5	Mandatory refresher course	12, 1
NSC6	Compliance audits	10, 1
NSC7	Screen Locks on PCs	5, 1, 7
NSC8	“Sensitive information not being stored on server” policy	11, 5
Security Control Related to Information Disclosure Vulnerabilities		
NSC9	Restricted version of mail utility	9, 7, 3,
NSC10	Use of Encrypting modems	7, 1, 3
NSC11	Corporate with mainframe agency to use encryption	1, 7
Security Control Related to Network Threats		
NSC12	VPN	
NSC13	DMZ	

MOT controls that are covered by current and proposed by new CISO, HGA controls, and VPN server and DMZ (Histogram)



Security Risk Prevention Strategy

Security Risk ($) Calculations for Assets with Vulnerabilities discovered by new CISO and protected by implementing and proposed controls by new CISO, missing MOT controls, and DMZ and VPN.

Assets Subsets:

Asset Representation	**Asset Description**	**Asset Value**
A1	Financial Resources	$500000
A3	Personal Information	$300000
A2.3	Routers	$5250
A2.5	LAN Servers	$35000

Vulnerability Subsets:

Vulnerability Representation	**Vulnerability Description**
V2	Unencrypted data transmission to/from server
V3	Master database stored in mainframe prone to attack
V5	Unauthorized Access
V11	Accidental Corruption and Loss of Data

Threat/Vulnerability Pairs along with *Reduced* likelihood probabilities in percentage:

	T1	**T2**	**T4**	**T8**
V2 on A1, A3, A2.3, & A2.5	8	16	7	9
V3 on A1, A3, A2.3, & A2.5	20	13	15	10
V5 on A1, A3, A2.3, & A2.5	12	14	11	12
V11 on A1, A3, A2.3, & A2.5	10	4	7	9

Initial Risk Impacts (100%, thus 0% Resilience for the worst-case scenario)

Threats exploiting Vulnerabilities.

Assets	T1*V2	T1*V3	T1*V5	T1*V11	T2*V2	T2*V3	T2*V5	T2*V11	T4*V2	T4*V3	T4*V5	T4*V11	T8*V2	T4*V3	T4*V5	T4*V11
A1	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%
A2.3	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%
A2.5	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%	100%

Calculate Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks

Asset Security Risk =

Asset Value (%) * Sum of threat/vulnerability probabilities

Sum of threat/vulnerability probabilities =
8 + 16 + 7 + 9 + 20 + 13 + 15+ 10 + 12 + 14 + 11 + 12 + 10 + 4 + 7 + 9 = 177

Risk of A1= $500000 * 177 = 171.69 > $500000

Thus, **Risk of A1** = $88500000 (total asset loss)

Risk of A3 = $300000 * 177 = 171.69 > $300000

Thus, **Risk of A3** = $53100000 (total asset loss)

Risk of A2.3 = $5250 * 177 = 166.38 > $5250

Thus, **Risk of A2.3** = $929250 (total asset loss)

Risk of A2.5 = $35000 * 177 = 166.38 > $35000

Thus, **Risk of A2.5** = $6195000 (total asset loss)

Residual Risk of All Assets = 97 + 97 + 94 + 94 = $840,250

Calculate Vulnerability Security Risks

Sum of V2 on A1, A3, A2.3, & A2.5 = 8 + 16 + 7 + 9 = 40
Sum of V3 on A1, A3, A2.3, & A2.5 = 20 + 13 + 15+ 10 = 58
Sum of V5 on A1, A3, A2.3, & A2.5 = 12 + 14 + 11 + 12 = 49
Sum of V11 on A1, A3, A2.3, & A2.5 = 10 + 4 + 7 + 9 = 30

Risk of V2: ($500000 *40) + ($300000 *40) + ($5250 *40) + ($35000 *40) = $33610000
Risk of V3: ($500000 *58) + ($300000 *58) + ($5250 *58) + ($35000 *58) = $48734500
Risk of V5: ($500000 *49) + ($300000 *49) + ($5250 *49) + ($35000 *49) = $41172250
Risk of V11: ($500000 *30) + ($300000 *30) + ($5250 *30) + ($35000 *30) = $25207500

Ranking of security asset residual risks with updated information

Rank	Security Asset
1	A1: Financial Resources
2	A3: Personal Information
3	A2.5: LAN servers
4	A2.3: Routers

Ranking of vulnerability security risks

Rank	Vulnerability
1	V3: Unauthorized Access
2	V5: Accidental Corruption and Loss of Data
3	V2: Unencrypted data transmission to/from server
4	V11: Master database stored in mainframe prone to attack

Security Risk Prevention Strategy I

List of missing MOT controls:

Some of the controls listed below were present and listed in HGA's list of controls however, they weren't fully adopted.

Management	**Operational**	**Technical**
Risk Management	Physical security	IAM – Identity Authentication
Life cycle	Contingency planning	Audit Trails
Security Plan	Data Integrity	Logical Access Control
Policies	Incident response plan	

With the installation of the DMZ and VPN Servers, number of Assets at HGA increased. HGA decided to add these two assets as they will increase the layers of security. DMZ will protect sensitive information from the outside world as it sits between what the Public can access with what Internal people can access. This creates a data filter hence enhanced level of security.

Thus:

VPN Server: $5000
DMZ: $150000

Information assets inventory with values

Assets Representation	**Assets Description**	**Asset Value**
A1	Financial resources	$500000
A2:	***System components***	
A2.1	PCs	$1500000
A2.2	Printers	$1800
A2.3	Routers	$5250
A2.4	Modem Pool	$3000
A2.5	LAN server	$35000
A2.6	Console	$5000
A2.7	VPN Server	$5000
A3	Personal Information	$300000
A4	Contracting & procurement document	$10000
A5	Draft regulations	$10000
A6	Business reports	$10000
A7:	***Intangible assets***	
A7.1	Reputation of agency	-
A7.2	Employee's confidence	-
A7.3	DMZ	$150000

Assets Subsets:

Asset Representation	Asset Description	Asset Value
A1	Financial Resources	$500000
A3	Personal Information	$300000
A2.3	Routers	$5250
A2.5	LAN Servers	$35000
A2.7	VPN	$5000
A7.3	DMZ	$150000

New Vulnerability due to VPN:

People can now login and access internal network remotely. Making it more vulnerable for attackers. Hence, creating a new Vulnerability "Remote Access" posing a threat of "Misusing of Resources" (T10).

Vulnerability Subsets:

Vulnerability Representation	Vulnerability Description
V2	Unencrypted data transmission to/from server
V3	Master database stored in mainframe prone to attack
V5	Unauthorized Access
V11	Accidental Corruption and Loss of Data
V17	Remote Access

Threat/Vulnerability Pairs along with *Reduced* likelihood probabilities in percentage:

	T1	T2	T4	T8	T10
V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3	8	16	7	9	20
V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3	20	13	15	10	10
V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3	12	14	11	12	30
V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	4	7	9	20
V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	10	15	20	10

Calculating Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks

Asset Security Risk =
Asset Value (%) * Sum of threat/vulnerability probabilities

Sum of threat/vulnerability probabilities =
8 + 16 + 7 + 9 + 20 + 13 + 15+ 10 + 12 + 14 + 11 + 12 + 10 + 4 + 7 + 9 + 20 + 10 + 30 + 20 + 10 + 10 + 10 + 15 + 20 = 322

Risk of A1= $500000 * 322 = $88500000 > $500000
Thus, **Risk of A1** = $88500000 (total asset loss)
Risk of A3 = $300000 * 322 = $53100000> $300000
Thus, **Risk of A3** = $53100000 (total asset loss)
Risk of A2.3 = $5250 * 322 = $929250 > $5250
Thus, **Risk of A2.3** = $929250 (total asset loss)
Risk of A2.5 = $35000 * 322 = 6195000> $35000
Thus, **Risk of A2.5** = $6195000 (total asset loss)
Risk of A2.7 = $5000* 322 = $1,610,000> $5000
Thus, **Risk of A2.7** = $1,610,000 (total asset loss)
Risk of A7.3 = $150000* 322 = $48,300,000> $150000
Thus, **Risk of A7.3** = $48,300,000 (total asset loss)

Residual Risk of All Assets = $995,250.00

Ranking of security asset residual risks with updated information

Rank	**Security Asset**
1	A1: Financial Resources
2	A3: Personal Information
3	A7.3: DMZ
4	A2.5: LAN servers
5	A2.3: Routers
6	A2.7: VPN

Calculate Vulnerability Security Risks

Sum of V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 8 + 16 + 7 + 9 + 20 = 60
Sum of V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 20 + 13 + 15+ 10 + 10 = 68
Sum of V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 12 + 14 + 11 + 12 + 30 = 79
Sum of V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 10 + 4 + 7 + 9 + 20 = 50
Sum of V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 10 + 10 + 15 + 20 + 10 = 65

Risk of V2: ($500000 *60) + ($300000 *60) + ($5250 *60) + ($35000 *60) + ($5000*60) + ($150000*60) = $59715000
Risk of V3: ($500000 *68) + ($300000 *68) + ($5250 *68) + ($35000 *68) + ($5000*68) + ($150000*68) = $67677000
Risk of V5: ($500000 *79) + ($300000 *79) + ($5250 *79) + ($35000 *79) + ($5000*79) + ($150000*79) = $78624750
Risk of V11: ($500000 *50) + ($300000 *50) + ($5250 *50) + ($35000 *50) + ($5000*50) + ($150000*50) = $49762500
Risk of V17: ($500000 *65) + ($300000 *65) + ($5250 *65) + ($35000 *65) + ($5000*65) + ($150000*65) = $64691250

Ranking of vulnerability security risks

Rank	**Vulnerability**
1	V5: Accidental Corruption and Loss of Data
2	V3: Unauthorized Access
3	V17: Remote Access
4	V2: Unencrypted data transmission to/from server
5	V11: Master database stored in mainframe prone to attack

Security Risk Prevention Strategy Step P2:

Apply additional Hardening Controls (for example 2-Factor Authentication) to highest ranked Vulnerability Risk, with further reduced probabilities, thus further reducing the overall security asset residual risk and create a new ranking of vulnerability security risks. In this step you need to include in the Asset inventory the value of points from the M-O-T Controls in Step P1 (!).

NOTE: Only reduce for Highest Ranked Vulnerability.
Paragraph explanation
"V5: Accidental Corruption and Loss of Data" was the highest vulnerability. Applied

Threat/Vulnerability pairs along with *Reduced* likelihood probabilities in percentage:

	T1	**T2**	**T4**	**T8**	**T10**
V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3	8	16	7	9	20
V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3	20	13	15	10	10
V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*7*	*4*	*6*	*7*	4
V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	4	7	9	20
V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	10	15	20	10

Calculating Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks

Asset Security Risk =

Asset Value (%) * Sum of threat/vulnerability probabilities

Sum of threat/vulnerability probabilities =
8 + 16 + 7 + 9 + 20 + 13 + 15+ 10 + 7 + 4 + 6 + 7 + 10 + 4 + 7 + 9 + 20 + 10 + 4 + 20 + 10 + 10 + 10 + 15 + 20 = 271

Risk of A1= $500000 * 271 = $135500000 > $500000
Thus, **Risk of A1** = $135500000 (total asset loss)
Risk of A3 = $300000 * 271 = $81300000 > $300000
Thus, **Risk of A3** = $81300000 (total asset loss)
Risk of A2.3 = $5250 * 271 = $1422750 > $5250
Thus, **Risk of A2.3** = $1422750 (total asset loss)
Risk of A2.5 = $35000 * 271 = $9485000 > $35000
Thus, **Risk of A2.5** = $9485000 (total asset loss)
Risk of A2.7 = $5000* 271 = $1355000 > $5000
Thus, **Risk of A2.7** = $1355000 (total asset loss)
Risk of A7.3 = $150000* 271 = $40650000 > $150000
Thus, **Risk of A7.3** = $40650000 (total asset loss)

Residual Risk of All Assets = $995,250.00

Ranking of security asset residual risks with updated information

Rank	Security Asset
1	A1: Financial Resources
2	A3: Personal Information
3	A7.3: DMZ
4	A2.5: LAN servers
5	A2.3: Routers
6	A2.7: VPN

Calculate Vulnerability Security Risks

Sum of V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 8 + 16 + 7 + 9 + 20 = 60
Sum of V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 20 + 13 + 15+ 10 + 10 = 68
Sum of V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 7 + 4 + 6 + 7 + 4 = 28
Sum of V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 10 + 4 + 7 + 9 + 20 = 50
Sum of V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 10 + 10 + 15 + 20 + 10 = 65

Risk of V2: ($500000 *60) + ($300000 *60) + ($5250 *60) + ($35000 *60) + ($5000*60) + ($150000*60) = $59715000
Risk of V3: ($500000 *68) + ($300000 *68) + ($5250 *68) + ($35000 *68) + ($5000*68) + ($150000*68) = $67677000
*Risk of V5: ($500000 *28) + ($300000 *28) + ($5250 *28) + ($35000 *28) + ($5000*28) + ($150000*28) = $27867000*
Risk of V11: ($500000 *50) + ($300000 *50) + ($5250 *50) + ($35000 *50) + ($5000*50) + ($150000*50) = $49762500
Risk of V17: ($500000 *65) + ($300000 *65) + ($5250 *65) + ($35000 *65) + ($5000*65) + ($150000*65) = $64691250

Ranking of vulnerability security risks

Rank	Vulnerability
1	V3: Unauthorized Access
2	V17: Remote Access
3	V2: Unencrypted data transmission to/from server
4	V11: Master database stored in mainframe prone to attack
5	*V5: Accidental Corruption and Loss of Data*

Security Risk Prevention Strategy Step P3:

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

NOTE: Only reduce for Highest Ranked Vulnerability.
Paragraph explanation
"V3: Unauthorized Access" was the highest vulnerability. Applied

Threat/Vulnerability pairs along with *Reduced* likelihood probabilities in percentage:

	T1	**T2**	**T4**	**T8**	**T10**
V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3	8	16	7	9	20
V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*4*	*2*	*5*	*6*	4
V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*7*	*4*	*6*	*7*	4
V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	4	7	9	20
V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	10	15	20	10

Calculating Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks

Asset Security Risk =

Asset Value (%) * Sum of threat/vulnerability probabilities

Sum of threat/vulnerability probabilities =
8 + 16 + 7 + 9 + 4 + 2 + 5+ 6 + 7 + 4 + 6 + 7 + 10 + 4 + 7 + 9 + 20 + 4 + 4 + 20 + 10 + 10 + 10 + 15 + 20 = 224

Risk of A1= $500000 * 224 = $135500000 > $500000

Thus, **Risk of A1** = $135500000 (total asset loss)

Risk of A3 = $300000 * 224= $81300000 > $300000

Thus, **Risk of A3** = $81300000 (total asset loss)

Risk of A2.3 = $5250 * 224 = $1422750 > $5250

Thus, **Risk of A2.3** = $1422750 (total asset loss)

Risk of A2.5 = $35000 * 224 = $9485000 > $35000

Thus, **Risk of A2.5** = $9485000 (total asset loss)

Risk of A2.7 = $5000* 224 = $1355000 > $5000

Thus, **Risk of A2.7** = $1355000 (total asset loss)

Risk of A7.3 = $150000* 224 = $40650000 > $150000

Thus, **Risk of A7.3** = $40650000 (total asset loss)

Residual Risk of All Assets = $995,250.00

Ranking of security asset residual risks with updated information

Rank	Security Asset
1	A1: Financial Resources
2	A3: Personal Information
3	A7.3: DMZ
4	A2.5: LAN servers
5	A2.3: Routers
6	A2.7: VPN

Calculate Vulnerability Security Risks

Sum of V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 8 + 16 + 7 + 9 + 20 = 60
Sum of V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 4 + 2 + 5 + 6 + 4 = 21
Sum of V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 7 + 4 + 6 + 7 + 4 = 28
Sum of V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 10 + 4 + 7 + 9 + 20 = 50
Sum of V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3 = 10 + 10 + 15 + 20 + 10 = 65

Risk of V2: ($500000 *60) + ($300000 *60) + ($5250 *60) + ($35000 *60) + ($5000*60) + ($150000*60) = $59715000
*Risk of V3: ($500000 *21) + ($300000 *21) + ($5250 *21) + ($35000 *21) + ($5000*21) + ($150000*21) = $20900250*
*Risk of V5: ($500000 *28) + ($300000 *28) + ($5250 *28) + ($35000 *28) + ($5000*28) + ($150000*28) = $27867000*
Risk of V11: ($500000 *50) + ($300000 *50) + ($5250 *50) + ($35000 *50) + ($5000*50) + ($150000*50) = $49762500
Risk of V17: ($500000 *65) + ($300000 *65) + ($5250 *65) + ($35000 *65) + ($5000*65) + ($150000*65) = $64691250

Ranking of vulnerability security risks

Rank	Vulnerability
1	V17: Remote Access
2	V2: Unencrypted data transmission to/from server
3	V11: Master database stored in mainframe prone to attack
4	V5: Accidental Corruption and Loss of Data
5	*V3: Unauthorized Access*

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

Current HGA controls along with the proposed controls by CISO were not sufficient. However, after introducing a VPN Server and a DMZ in the system, it became more secured. Granted we can make it even better by implementing more controls to reduce the security risk for HGA.

Security Risk Response (Resilience) Strategy Step R1:

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

Management	**Operational**	**Technical**
Policies	Trainings and education	Access Control
	Incident Handling	

Threat/Vulnerability pairs along from step P3:

	T1	**T2**	**T4**	**T8**	**T10**
V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3	8	16	7	9	20
V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*4*	*2*	*5*	*6*	4
V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*7*	*4*	*6*	*7*	4
V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	4	7	9	20
V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	10	15	20	10

Updated Risk Impacts

Assets	**T1*V2**	**T1*V3**	**T1*V5**	**T1*V11**	**T1*V17**	**T2*V2**	**T2*V3**	**T2*V5**	**T2*V11**	**T2*V17**	**T4*V2**	**T4*V3**
A1	20%	40%	30%	50%	20%	30%	40%	20%	50%	40%	40%	20%
A3	30%	50%	30%	30%	30%	40%	20%	20%	30%	20%	20%	40%
A2.3	50%	20%	20%	20%	50%	30%	20%	50%	20%	20%	40%	30%
A2.5	40%	30%	40%	50%	40%	20%	30%	30%	40%	30%	50%	20%
A2.7	20%	40%	30%	50%	30%	40%	20%	20%	50%	40%	40%	20%

T4*V5	**T4*V11**	**T4*V17**	**T8*V2**	**T8*V3**	**T8*V5**	**T8*V11**	**T8*V17**	**T10*V2**	**T10*V3**	**T10*V5**	**T10*V11**	**T10*V17**
30%	20%	30%	50%	40%	30%	30%	30%	30%	40%	20%	50%	40%
50%	30%	50%	40%	20%	40%	20%	20%	40%	20%	20%	30%	20%
20%	20%	20%	30%	20%	20%	30%	30%	30%	20%	50%	20%	20%
40%	30%	40%	50%	30%	40%	50%	50%	20%	30%	30%	40%	30%
30%	30%	50%	40%	20%	40%	20%	20%	40%	20%	20%	50%	40%

Calculating Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks with Updated Information

Risk of A1:
$500000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $800075.7 < $500000
Therefore, partial asset loss is $800074.7

Risk of A3:
$300000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $720067.9< $300000
Therefore, partial asset loss is $720067.9

Risk of A2.3:
$5250*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $21057.9 < $5250
Therefore, partial asset loss is $21057.9

Risk of A2.5:
$35000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $ 112078.6 > $35000
Therefore, No Asset loss

Residual Risk of All Assets = $112078.6

Risk of A2.7:
$5000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $ 8077.5 > $5000
Therefore, No Asset loss
Residual Risk of All Assets = $8077.5

Ranking of security asset residual risks with updated information

Rank	Security Asset
1	A1: Financial Resources
2	A3: Personal Information
3	A2.5: LAN servers
4	A2.3: Routers
5	A2.7: VPN

Calculate Vulnerability Security Risks with Updated Information

Risk of V2:
($500000*(8*20+16*30+7*40+9*50+20*20))+($300000*(8*30+16*40+7*20+9*40+20*40))+(
$5250*(8*50+16*30+7*40+9*30+20*40))+(
$35000*(8*40+16*20+7*50+9*50+20*40)))+(
$5000*(8*40+16*20+7*50+9*50+20*40))) = $ 1688892

Risk of V3:
($500000*(4*40+2*40+5*20+6*40+6*40))+(
$300000*(4*50+2*20+5*40+6*20+6*20))+(
$5250*(4*20+2*20+5*30+6*20+6*20))+(
$35000*(4*30+2*30+5*20+6*30+6*20)))+(
$5000*(4*30+2*30+5*20+6*30+6*20))) = $ 1348221.7

Risk of V5:
($500000*(7*30+4*20+6*30+7*30+4*30))+(
$300000*(7*30+4*20+6*50+7*40+4*20))+))+(
$5250*(7*20+4*50+6*20+7*20+4*30))+(
$35000*(7*40+4*30+6*40+7*40+4*40))+(
$5000*(7*40+4*30+6*40+7*40+4*20)))) = $ 1561559.2

Risk of V11:
($500000*(10*50+4*50+7*20+9*30+20*50))+(
$300000*(10*30+4*30+7*30+9*20+20*50))+))+(
$5250*(10*20+4*20+7*20+9*30+20*30))+(
$35000*(10*50+4*40+7*30+9*50+20*20)))+(
$5000*(10*50+4*40+7*30+9*50+20*50))) = $ 4140572.2

Risk of V17:
($500000*(10*50+10*50+15*20+20*30+10*30))+(
$300000*(10*30+10*30+15*30+20*20+10*40))+))+(
$5250*(10*20+10*20+15*20+20*30+10*50))+(
$35000*(10*50+10*40+15*30+20*50+10*20)))+(
$5000*(10*50+10*40+15*30+20*50+10*40))) = $ 2340841

Ranking of vulnerability security risks with updated information

Rank	Vulnerability
1	V11: Master database stored in mainframe prone to attack
2	V17: Remote Access
3	V2: Unencrypted data transmission to/from server
4	V5: Accidental Corruption and Loss of Data

5	V3: Unauthorized Access

Security Risk Response (Resilience) Strategy Step R2:

Apply additional Hardening Controls (for example restricting services or adding a redundant server) to highest ranked Residual Asset Risk, thus further reducing risk impact probabilities, and further reducing the overall security asset residual risk and create a new ranking of vulnerability security risks. In this step you need to include in the Asset inventory the value of points from the M-O-T Controls in Step R1 (!).

A1: Financial Resources highest ranked asset.

Threat/Vulnerability pairs along from step P3:

	T1	**T2**	**T4**	**T8**	**T10**
V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3	8	16	7	9	20
V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*4*	*2*	*5*	*6*	4
V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*7*	*4*	*6*	*7*	4
V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	4	7	9	20
V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	10	15	20	10

Updated Risk Impacts

Assets	**T1*V2**	**T1*V3**	**T1*V5**	**T1*V11**	**T1*V17**	**T2*V2**	**T2*V3**	**T2*V5**	**T2*V11**	**T2*V17**	**T4*V2**	**T4*V3**
A1	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*
A3	30%	50%	30%	30%	30%	40%	20%	20%	30%	20%	20%	40%
A2.3	50%	20%	20%	20%	50%	30%	20%	50%	20%	20%	40%	30%
A2.5	40%	30%	40%	50%	40%	20%	30%	30%	40%	30%	50%	20%
A2.7	20%	40%	30%	50%	30%	40%	20%	20%	50%	40%	40%	20%

T4*V5	**T4*V11**	**T4*V17**	**T8*V2**	**T8*V3**	**T8*V5**	**T8*V11**	**T8*V17**	**T10*V2**	**T10*V3**	**T10*V5**	**T10*V11**	**T10*V17**
10%	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*
50%	30%	50%	40%	20%	40%	20%	20%	40%	20%	20%	30%	20%

20%	20%	20%	30%	20%	20%	30%	30%	30%	20%	50%	20%	20%
40%	30%	40%	50%	30%	40%	50%	50%	20%	30%	30%	40%	30%
30%	30%	50%	40%	20%	40%	20%	20%	40%	20%	20%	50%	40%

Calculating Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks with Updated Information

Risk of A1:

$500000(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $400,021.6 < $500,000*

Therefore, partial asset loss is $400021.6

Risk of A3:

$300000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $720067.9< $300000

Therefore, partial asset loss is $720067.9

Risk of A2.3:

$5250*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $21057.9 < $5250

Therefore, partial asset loss is $21057.9

Risk of A2.5:

$35000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $ 112078.6 > $35000

Therefore, No Asset loss

Residual Risk of All Assets = $112078.6

Risk of A2.7:

$5000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $ 8077.5 > $5000

Therefore, No Asset loss

Residual Risk of All Assets = $8077.5

Ranking of security asset residual risks with updated information

Rank	Security Asset
1	A3: Personal Information
2	A1: Financial Resources

3	A2.5: LAN servers
4	A2.3: Routers
5	A2.7: VPN

Calculate Vulnerability Security Risks with Updated Information

Risk of V2:

($500000*(8*10+16*30+7*40+9*50+20*20))+($300000*(8*10+16*40+7*20+9*40+20*40))+(
$5250*(8*10+16*30+7*40+9*30+20*40))+(
$35000*(8*10+16*20+7*50+9*50+20*40)))+(
$5000*(8*10+16*20+7*50+9*50+20*40))) = $ 676292

Risk of V3:

($500000*(4*10+2*40+5*20+6*40+6*40))+(
$300000*(4*10+2*20+5*40+6*20+6*20))+(
$5250*(4*10+2*20+5*30+6*20+6*20))+(
$35000*(4*10+2*30+5*20+6*30+6*20)))+(
$5000*(4*10+2*30+5*20+6*30+6*20))) = $ 338121.7

Risk of V5:

($500000*(7*10+4*20+6*30+7*30+4*30))+(
$300000*(7*10+4*20+6*50+7*40+4*20))+))+(
$5250*(7*10+4*50+6*20+7*20+4*30))+(
$35000*(7*10+4*30+6*40+7*40+4*40))+(
$5000*(7*10+4*30+6*40+7*40+4*20)))) = $ 591709.2

Risk of V11:

($500000*(10*10+4*50+7*20+9*30+20*50))+(
$300000*(10*10+4*30+7*30+9*20+20*50))+))+(
$5250*(10*10+4*20+7*20+9*30+20*30))+(
$35000*(10*10+4*40+7*30+9*50+20*20)))+(
$5000*(10*10+4*40+7*30+9*50+20*50))) = $ 845322.2

Risk of V17:

($500000*(10*10+10*50+15*20+20*30+10*30))+(
$300000*(10*10+10*30+15*30+20*20+10*40))+))+(
$5250*(10*10+10*20+15*20+20*30+10*50))+(
$35000*(10*10+10*40+15*30+20*50+10*20)))+(
$5000*(10*10+10*40+15*30+20*50+10*40))) = $ 845341

Ranking of vulnerability security risks with updated information

Rank	Vulnerability
1	V17: Remote Access
2	V11: Master database stored in mainframe prone to attack
3	V2: Unencrypted data transmission to/from server
4	V5: Accidental Corruption and Loss of Data
5	V3: Unauthorized Access

Security Risk Response (Resilience) Strategy Step R3:

Apply additional Hardening Controls to new now highest ranked Residual Asset Risk, thus reducing risk impact probabilities, and further reducing the overall security asset residual risk and create a new ranking of vulnerability security risks. In this step you need to include the value of points from the Hardening Controls in Step R2 in the Asset inventory (!) and increase asset risk loss (for example by restriction of services impacting operational effectiveness or possibly total loss of the asset, but not the service, that has a redundant back-up).

A3: Personal Information is the highest ranked asset
Threat/Vulnerability pairs along from step P3:

Threat/Vulnerability pairs along from step P3:

	T1	T2	T4	T8	T10
V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3	8	16	7	9	20
V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*4*	*2*	*5*	*6*	4
V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*7*	*4*	*6*	*7*	4
V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	4	7	9	20
V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	10	15	20	10

Updated Risk Impacts

Assets	T1*V2	T1*V3	T1*V5	T1*V11	T1*V17	T2*V2	T2*V3	T2*V5	T2*V11	T2*V17	T4*V2	T4*V3
A1	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A3	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*
A2.3	50%	20%	20%	20%	50%	30%	20%	50%	20%	20%	40%	30%
A2.5	40%	30%	40%	50%	40%	20%	30%	30%	40%	30%	50%	20%
A2.7	20%	40%	30%	50%	30%	40%	20%	20%	50%	40%	40%	20%

T4*V5	T4*V11	T4*V17	T8*V2	T8*V3	T8*V5	T8*V11	T8*V17	T10*V2	T10*V3	T10*V5	T10*V11	T10*V17
10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
20%	20%	20%	30%	20%	20%	30%	30%	30%	20%	50%	20%	20%
40%	30%	40%	50%	30%	40%	50%	50%	20%	30%	30%	40%	30%
30%	30%	50%	40%	20%	40%	20%	20%	40%	20%	20%	50%	40%

Calculating Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks with Updated Information

Risk of A1:
$500000*(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $400,021.6 < $500,000
Therefore, partial asset loss is $400021.6

Risk of A3:
$300000(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $240021.6< $300000*
Therefore, partial asset loss is $240021.6

Risk of A2.3:
$5250*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $21057.9 < $5250
Therefore, partial asset loss is $21057.9

Risk of A2.5:
$35000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $ 112078.6 > $35000
Therefore, No Asset loss
Residual Risk of All Assets = $112078.6

Risk of A2.7:
$5000*(8*20+4*40+7*30+10*50+10*30+16*40+2*20+4*50+4*40+10*20+7*30+5*20+6*50+7*40+15*30+9*30+6*20+7*40+9*30+20*50+20*30+4*40+4*20+20*50+10*40) = $ 8077.5 > $5000

Therefore, No Asset loss
Residual Risk of All Assets = $8077.5

Ranking of security asset residual risks with updated information

Rank	Security Asset
1	A1: Financial Resources
2	A3: Personal Information
3	A2.5: LAN servers
4	A2.3: Routers
5	A2.7: VPN

Calculate Vulnerability Security Risks with Updated Information

Risk of V2:
($500000*(8*10+16*10+7*40+9*50+20*20))+($300000*(8*10+16*10+7*20+9*40+20*40))+(
$5250*(8*10+16*10+7*40+9*30+20*40))+(
$35000*(8*10+16*10+7*50+9*50+20*40)))+(
$5000*(8*10+16*10+7*50+9*50+20*40))) = $ 676272.8

Risk of V3:
($500000*(4*10+2*10+5*20+6*40+6*40))+(
$300000*(4*10+2*10+5*40+6*20+6*20))+(
$5250*(4*10+2*10+5*30+6*20+6*20))+(
$35000*(4*10+2*10+5*20+6*30+6*20)))+(
$5000*(4*10+2*10+5*20+6*30+6*20))) = $ 338119.7

Risk of V5:
($500000*(7*10+4*10+6*30+7*30+4*30))+(
$300000*(7*10+4*10+6*50+7*40+4*20))+))+(
$5250*(7*10+4*10+6*20+7*20+4*30))+(
$35000*(7*10+4*10+6*40+7*40+4*40))+(
$5000*(7*10+4*10+6*40+7*40+4*20)))) = $ 591704.8

Risk of V11:
($500000*(10*10+4*10+7*20+9*30+20*50))+(
$300000*(10*10+4*10+7*30+9*20+20*50))+))+(
$5250*(10*10+4*10+7*20+9*30+20*30))+(
$35000*(10*10+4*10+7*30+9*50+20*20)))+(
$5000*(10*10+4*10+7*30+9*50+20*50))) = $ 845318.6

Risk of V17:
($500000*(10*10+10*10+15*20+20*30+10*30))+(
$300000*(10*10+10*10+15*30+20*20+10*40))+))+(
$5250*(10*10+10*10+15*20+20*30+10*50))+(

$35000*(10*10+10*10+15*30+20*50+10*20)))+(
$5000*(10*10+10*10+15*30+20*50+10*40))) = $ 845332

Ranking of vulnerability security risks with updated information

Rank	Vulnerability
1	V17: Remote Access
2	V11: Master database stored in mainframe prone to attack
3	V2: Unencrypted data transmission to/from server
4	V5: Accidental Corruption and Loss of Data
5	V3: Unauthorized Access

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

At this point, current list of controls plus CISO proposed controls with VPN and DMZ provides a secured environment for HGA. But HGA's security system can still be improved by implementing new measures or controls.
In terms of common criteria, after the risk assessment, both management controls, operational controls and technical controls have improved drastically. Making sure the system is current, daily operations are monitored and secured using IDS and IPS etc.

Mixed Security Risk Prevention Strategy and Security Risk Response Strategy

Threat/Vulnerability pairs along from step P3:

	T1	**T2**	**T4**	**T8**	**T10**
V2 on A1, A3, A2.3, A2.5, A2.7, & A7.3	8	16	*7*	9	*20*
V3 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*4*	*2*	*5*	*6*	4
V5 on A1, A3, A2.3, A2.5, A2.7, & A7.3	*7*	*4*	*6*	*7*	4
V11 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	4	7	9	*20*
V17 on A1, A3, A2.3, A2.5, A2.7, & A7.3	10	10	15	*20*	10

Updated Risk Impacts

Assets	**T1*V2**	**T1*V3**	**T1*V5**	**T1*V11**	**T1*V17**	**T2*V2**	**T2*V3**	**T2*V5**	**T2*V11**	**T2*V17**	**T4*V2**	**T4*V3**	**T4*V5**	**T4*V11**
A1	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A3	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
A2.3	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*
A2.5	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*
A2.7	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*

T4*V5	**T4*V11**	**T4*V17**	**T8*V2**	**T8*V3**	**T8*V5**	**T8*V11**	**T8*V17**	**T10*V2**	**T10*V3**	**T10*V5**	**T10*V11**	**T10*V17**
10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%	10%
20%	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*
40%	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*
30%	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*	*10%*

Calculating Residual Asset Security Risks and Vulnerability Security Risks:

Calculate Residual Asset Security Risks with Updated Information

Risk of A1:
$500000*(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $400018.6< $500,000
Therefore, partial asset loss is $400018.6

Risk of A3:
$300000*(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $240018.6< $300000
Therefore, partial asset loss is $240018.6

Risk of A2.3:
$5250*(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $4218.6< $5250
Therefore, partial asset loss is $4218.6

Risk of A2.5:
$35000*(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $ 28018.6> $35000
Therefore, No Asset loss
Residual Risk of All Assets = $28018.6

Risk of A2.7:
$5000*(8*10+4*10+7*10+10*10+10*10+16*10+2*10+4*10+4*10+10*10+7*10+5*10+6*10+7*10+15*10+9*10+6*10+7*10+9*10+20*10+20*10+4*10+4*10+20*10+10*10) = $ 4018.6> $5000
Therefore, No Asset loss
Residual Risk of All Assets = $4018.6

Ranking of security asset residual risks with updated information

Rank	Security Asset
1	A1: Financial Resources
2	A3: Personal Information
3	A2.5: LAN servers
4	A2.3: Routers
5	A2.7: VPN

Calculate Vulnerability Security Risks with Updated Information

Risk of V2:
($500000*(8*10+16*10+7*10+9*10+20*10))+($300000*(8*10+16*10+7*10+9*10+20*10))+(
$5250*(8*10+16*10+7*10+9*10+20*10))+(
$35000*(8*10+16*10+7*10+9*10+20*10)))+(
$5000*(8*10+16*10+7*10+9*10+20*10))) = $ 676221

Risk of V3:
($500000*(4*10+2*10+5*10+6*10+6*10))+(
$300000*(4*10+2*10+5*10+6*10+6*10))+(
$5250*(4*10+2*10+5*10+6*10+6*10))+(
$35000*(4*10+2*10+5*10+6*10+6*10)))+(
$5000*(4*10+2*10+5*10+6*10+6*10))) = $ 338108.5

Risk of V5:
($500000*(7*10+4*10+6*10+7*10+4*10))+(
$300000*(7*10+4*10+6*10+7*10+4*10))+))+(
$5250*(7*10+4*10+6*10+7*10+4*10))+(
$35000*(7*10+4*10+6*10+7*10+4*10))+(
$5000*(7*10+4*10+6*10+7*10+4*10)))) = $ 591685.5

Risk of V11:
($500000*(10*10+4*10+7*10+9*10+20*10))+(
$300000*(10*10+4*10+7*10+9*10+20*10))+))+(
$5250*(10*10+4*10+7*10+9*10+20*10))+(
$35000*(10*10+4*10+7*10+9*10+20*10)))+(
$5000*(10*10+4*10+7*10+9*10+20*10))) = $ 845265

Risk of V17:
($500000*(10*10+10*10+15*10+20*10+10*10))+(
$300000*(10*10+10*10+15*10+20*10+10*10))+))+(
$5250*(10*10+10*10+15*10+20*10+10*10))+(
$35000*(10*10+10*10+15*10+20*10+10*10)))+(
$5000*(10*10+10*10+15*10+20*10+10*10))) = $ 845272.5

Ranking of vulnerability security risks with updated information

Rank	Vulnerability
1	V17: Remote Access
2	V11: Master database stored in mainframe prone to attack
3	V2: Unencrypted data transmission to/from server
4	V5: Accidental Corruption and Loss of Data
5	V3: Unauthorized Access

Conclusion: Cost Benefit Analysis

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

The HGA team have addressed a good amount of listed risk from the assessment based on their budget and supporting environment. Can they do better? Yes. But they are currently better off prior to the assessment.

At HGA, risk was assessed from time to time. Not enough as what security experts would recommend. It was only after the CISO introduced new policies that HGA did a considerate amount of period assessment. Initially not all Managers and employees at HGA were fully aware of the risk that the daily used software and programs could cause to the organization. After new policies were out in place, they were all trained to be aware. Yes, security controls of their system and interconnected systems have been reviewed. HGA works along with other external organizations to ensure their systems have been reviewed and are secured. HGA does not have a development life cycle methodology nor are their system certified. Yes, systems are operating on an interim authority processing accordingly to their organizational requirements. After new CISO, HGA security systems were fully reviewed, analyzed, and properly documented accordingly. One of the new policies was to ensure the system is kept current.

HGA enforces access control by ensuring individuals have proper permissions to access what they solely need for their roles. Prior to being hired at HGA, they ensure that people go through background screening. Physical security was one of their potential vulnerabilities, prior to new policies. However, this was resolved when new policies were put in place. Among the new policies, HGA focused on ensuring unauthorized individuals do not get inContact with any of their assets being restricted rooms, classified data, physical devices etc. They also ensured data to and from the server was properly secured. No interception. User support and media controls are now available at HGA. In their initial report, they identified their most critical operations and how much of a high value they are to their organization. They do have a contingency plan that was developed with the new CISO. Access to software and hardware are limited to both people working internally and outsiders. HGA works alongside with other companies/organizations. They ensure that those companies have such policies in place.

Currently, systems are HGA are managed to reduce vulnerabilities by actively monitoring the systems for viruses or any other suspicious activities. This is done using IDS – Intrusion detection systems. Documentations for such policies are available and safely stored. All security policies that were put in place after the risk analysis, were properly documented and stored for future references. HGA needs to work on Incident response planning. They do not have good plan put in place.

Authentication is enforced at HGA. They have policies that ensure users have unique strong password that must be changed frequently. Yes, access controls are enforcing separation of duties. Only Clarks can make changes to timesheets. The use of logical access control ensures unexpected transactions and functions are restricted prior to any damage to their organization. When public users access the system, due to limited access controls, they cannot modify HGA's applications or systems. On the other hand, there are controls put in place to ensure that such activities are detected.

Do you recommend a Risk Prevention Strategy, a Risk Response Strategy, or a mixed strategy as combination of both?

Risk prevention strategy focuses on reducing risk through vulnerability rankings. Thus, new security measures and policies are created that will reduce the risks on the highest ranked vulnerabilities. While response strategy focuses on reducing risk through assets rankings. Highest ranked assets are safeguarded first. This report has proven that the application of both strategies at once makes a better security strategy. We can reduce risk at a higher rate by using both strategies at once. Thus, I recommend the use of both strategies when feasible.

Does the Residual Risk Reduction exceed the budget for proposed controls?

Controls	**Risk Prevention Budget**	**Risk Response Budget**	**Mixed Budget or Proposal**
Controls for Payroll Fraud Vulnerability	$70,000	$80,000	$100,000
Controls for Payroll Error Vulnerability	$40,000	$25,000	$120,000
Controls for Payroll Information disclosure Vulnerability	$45,000	$25,000	$120,000
Controls for Payroll Network issue Vulnerability	$50,000	$50,000	$70,000
Review of security controls	$30,000	$30,000	$30,000
VPN	$2,000	$5,000	$6,000
DMZ	$50,000	$60,000	$100,000
Total	**$287,00**	**$275,00**	**$546,00**

Residual Risk Reduction:

= Residual Risk with current controls – Residual risk with new controls
= 845250 – 676293
=168,957
The value of residual risk reduction does not exceed the budget for the proposed controls

What is the ((proposed security risk budget cost)/ (expected security risk Benefit)) ratio for the 3 budgets from Mixed Strategy?

Cost benefit ratio analysis for risk prevention budget
=Proposed security risk budget cost/ expected security risk Benefit
=287,00/168,957
=1.70

Cost benefit ratio analysis for risk response budget
=Proposed security risk budget cost/ expected security risk Benefit
=275,00/168,957
=1.63

Cost benefit ratio analysis for Mixed budget
=Proposed security risk budget cost/ expected security risk Benefit
= 546,00/168,957
=3.23

PART B: Security Risk Management Implementation Plan

1. Access Control Security Risk Management Implementation Controls and Policies
    - Identification Credentials
    - Personal Authentication
    - Authorization
    - Logical Access Control Methods
    - Physical Access Control Methods
    - Biometric Systems

List of critical assets

Asset	Asset Type	Value ($)
A1	Application	$1000000
A2	Information Systems	$750000
A3	Financial Resources	$250000
A4	System Design	$100000
A5	Reputation	Intangible

List of missing Cybersecurity Implementation Controls

Missing controls
Identification credentials
Photograph
Personal authentication
Smart Card
Privilege token database
Limit Password Retires
Authorization
Deny by default policy
Logical access control method
DoD common access card as hardware token
Physical access control methods
CAC and defense biometric identification system for physical access control
Memory card

List of Potential Vulnerabilities:

1. Permanent tokens vulnerability
2. Unauthorized Access
3. Weak Authentication
4. Network based attacks
5. Impersonation – Brute force attack
6. Identity theft

List of Potential Threats:

1. Lack of data integrity
2. lack of service (availability)
3. exposure of confidential information
4. Spoofing
5. Damage reputation

List of potential Risk

1. Exposure of Confidential Information
2. Denial of Service – Users can't access application
3. Unauthorized access due to weak authentication
4. Impersonation of privileged personnel
5. Attack Network system both application and website

2. Network Infrastructure Security Risk Management Implementation Controls and Policies

- Enclave Protection
- Firewalls
- Routers

List of critical assets

Asset	**Asset Type**	**Value ($)**
A1	Application	$1000000
A2	Information Systems	$750000
A3	Financial Resources	$250000
A4	System Design	$100000
A5	Reputation	Intangible

List of missing Cybersecurity Implementation Controls

Missing controls
Enclave Protection
Enclave DMZ
Wireless Intrusion Detection System
Network Test Access Ports
Anti-Backdoor
Firewalls
Bastion Host
Deep Packet Inspection
Routers
Secure Router Planes

List of Potential Vulnerabilities:

1. Network Attacks
2. Unauthorized access
3. Backdoor attack
4. Increases chances of penetration
5. Botnet attack

List of Potential Threats:

1. No service
2. Loss of data integrity
3. No confidentiality
4. Destroyed application

List of potential Risk

1. Exposure of confidential Information
2. Availability of Service
3. Man in the Middle attacks
4. Redirection of traffic
5. Application attack

3. Network Infrastructure Management Security Risk Management Implementation Controls and Policies

- Ports, Protocols and Services
- Device Management
- Device Monitoring
- Network Authentication, Authorization, and Accounting (Auditing)
- Network Intrusion Detection Systems
- Switches and VLANs
- VPN

List of critical assets

Asset	**Asset Type**	**Value ($)**
A1	Application	$1000000
A2	Information Systems	$750000
A3	Financial Resources	$250000
A4	System Design	$100000
A5	Reputation	Intangible

List of missing Cybersecurity Implementation Controls

Missing controls
Ports, Protocols and Services
Updating Access List Rules
Unicast Reverse Path Forwarding
Switches, VLANs
VLAN Trunking
VPN
Gateway-to-gateway:
Host-to-host

List of Potential Vulnerabilities:

1. Network Attacks
2. Unauthorized access
3. IP Spoofing
4. ARP Attack
5. DoS – Denial of Service

List of Potential Threats:

1. No service
2. Loss of data integrity
3. No confidentiality
4. Destroyed application

List of potential Risk

1. Exposure of confidential Information
2. Availability of Service due to DoS
3. Man in the Middle attacks
4. Redirection of traffic
5. Application attack

4. Database Security Risk Management Implementation Controls and Policies

- Authentication
- Authorization
- Confidentiality
- Data Integrity
- Auditing
- Replication and Federation

- Clustering
- Backup and Recovery
- OS Protections
- Application Protections
- Network Protections
- Security Design and Configuration
- Enclave and Computing Environment
- Business Continuity
- Vulnerability and Incident Management

List of critical assets

Asset	**Asset Type**	**Value ($)**
A1	Application	$1000000
A2	Information Systems	$750000
A3	Financial Resources	$250000
A4	System Design	$100000
A5	Reputation	Intangible

List of missing Cybersecurity Implementation Controls

Missing Controls
Authentication – User accounts
Application User Manager
Application Account
Database Operator
External Authentication
Authorization
Renaming Default accounts
OS Protections
Dedicated OS account
Network Protections
Time and count limits
Security Design and Configuration
Security Structure Support Partitioning
Enclave and Computing environment
Audit Reduction and Report Generation
Remote Access for Privileged Functions

List of Potential Vulnerabilities:

1. Network Attacks
2. Unauthorized access
3. Application layer attacks
4. OS attacks
5. DoS – Denial of Service

List of Potential Threats:

1. No service
2. Loss of data integrity
3. No confidentiality
4. Destroyed application

List of potential Risk

1. Exposure of confidential Information
2. Availability of Service due to DoS
3. Undetected attacks
4. Application attack

5. Applications Development Security Risk Management Implementation Controls and Policies

- Application Data Handling
- Authentication
- Use of Cryptography
- User Accounts
- Input Validation
- Auditing
- Configuration Management
- Testing
- Deployment

List of critical assets

Asset	**Asset Type**	**Value ($)**
A1	Application	$1000000
A2	Information Systems	$750000
A3	Financial Resources	$250000
A4	System Design	$100000
A5	Reputation	Intangible

List of missing Cybersecurity Implementation Controls

Missing Controls
Application Data Handling
Data Marking
Authentication
Signed Code Identification
Combination Client Server Application Authentication
Application Component Authentication
User Accounts
No duplicate accounts
Input Validation
Use of Static Analysis Tools
Race Conditions
Configuring Management
Limit Unauthorized Individuals

List of Potential Vulnerabilities:

1. Network Attacks
2. Unauthorized access
3. Application layer attacks
4. DoS – Denial of Service
5. Exposure of confidential Information

List of Potential Threats:

1. No service
2. Loss of data integrity
3. No confidentiality
4. Destroyed application

List of potential Risk

1. Exposure of confidential Information
2. Availability of Service due to DoS
3. Undetected attacks
4. Application attack

5. Wireless Security Risk Management Implementation Controls and Policies

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

List of critical assets

Asset	Asset Type	Value ($)
A1	Application	$1000000
A2	Information Systems	$750000
A3	Financial Resources	$250000
A4	System Design	$100000
A5	Reputation	Intangible

List of missing Cybersecurity Implementation Controls

Missing Controls
Wireless LAN Risk Management
EAP-Tunneling Transport Layer Security
Protected Extensible Authentication Protocol (PEAP)
Broadcasting Service Set Identifier (SSID)
Wireless WAN Risk Management
Use of Cellular Digital Packet Data (CDPD)
Wireless RFID Risk Management
RFID Tag Encryption
Wireless PED Risk Management
PDA Security

List of Potential Vulnerabilities:

1. Network Attacks
2. Unauthorized access
3. Sniffing
4. Exposure of confidential Information
5. DoS – Denial of Service
6. Phishing

List of Potential Threats:

1. No service
2. Loss of data integrity
3. No confidentiality
4. Destroyed application

List of potential Risk

1. Exposure of confidential Information
2. Availability of Service due to DoS
3. Undetected attacks
4. Identity can be spoofed

List of Cybersecurity Implementation Controls that exist at GrubHub

Access Control Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation controls
Identification credentials
ID Card
Password
Digital signature
PINs
PKI certificate
Biometrics
Personal authentication
Password
Private key
Biometrics
Access Control List
Policies
Authorization
Access Control List
Security token
Logical access control method
Network architecture controls
Remote network access
Securing network ports
Physical security for Secure Internet Protocol Router Network (SIPRNeT) Ports
Logical network port security
Port authentication using 802.1x
Network access control (NAC) system
Encryption

PKI compliance requirements
Password
PINs
Implementing Something you know
Physical access control methods
Classified storage and handling
Attended access
Badges
Smart card
PINs, combinations, and other forms of something you know
Physical tokens
Physical intrusion detection systems
Biometric systems
Fingerprint scanner
Facial recognition

Network Infrastructure Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation controls
Enclave Protection
Defense-in-depth
Firewall
Router
IDS and IPS
Encryption
VPN tunnel
Firewalls
Packet Filters
Stateful Inspection
Application Proxy Gateway
Hybrid Technology Firewalls
Proxy Servers
Routers
Router Table Integrity

Network Infrastructure Management Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation controls
Ports, Protocols and Services
Blocking Protocols at the enclave perimeter
Blocking ICMPv4 Echo Request, Echo Reply and Redirect Packets
Disable Traceroute
IPv4 Address Filtering
SYN Flood attacks
Device Management
Device and Asset Management
Out-of-band Management
In-band Management
Device Monitoring
SNMP
Network Management Station
Network Authentication, Authorization, and Accounting (Auditing)
Authentication
Authorization
Accounting
Auditing
Router Password Protection
NIDS – Network Intrusion Detection System
External Network Intrusion Detection
External Network Intrusion Detection
Switches, VLANs
Physical
Virtual Local Area Networks
VLAN Port Security
802.1x and Management Policy Server
VPN
Host-to-gateway:

Database Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls
Authentication – User accounts
Application User
Database Administrator
Application Owner
Database Auditor
Passwords
Certificates
External Authentication

Credential Storage
Authorization
Role Based Access Control
Confidentiality
Data Encryption
Application Code Encryption
Data File Encryption:
Data Integrity
Transaction Log
Data Integrity
Auditing
Audit Logs Protection
Audit Logs Retention
Audit Reporting
Replication and Federation
Database
Database Replication
Clustering
Database Clustering
Least Privilege
Protected Communication Path
Backup and Recovery
DBMS Backup
Testing and Maintenance
Authentication and Authorization
OS Protections
Dedicated Directories and Files
Updated Database Software
Application Protections
Audit Elevated Privileges
Input Validation
Authentication Methods
Least Privilege Mechanism
Network Protections
Network Access
Time and count limits
Encrypted and protected data across network
Security Design and Configuration
Procedural Review
Configuration Specifications
Compliance Testing
Functional Architecture for IS Applications
Non-repudiation
Partitioning the application

Ports, protocols, and services
Configuration Management Process
IA Documentation
System Library Management Controls
System State Changes
Software Baseline
Group Identification and Authentication
Individual Identification and Authentication
Key Management
Token and Certificate Standards
Enclave and Computing environment
Access for Need to Know
Audit Record Content
Audit Trail, Monitoring, Analysis and Reporting
Changes to Data
Encryption for Confidentiality
Data Change Controls
Interconnections among Systems and Enclaves
Audit of Security Label Changes
Logon
Privileged Account Control
Marketing and Labelling
Production Code Change Controls
Resource Control
Security Configuration Compliance
Software Development Change Controls
Warning message
Boundary Defense
Remote Access for Privileged Functions
Business and Continuity
Protection of Backup and Restoration Assets
Data Backup Procedures
Disaster and Recovery Planning
Backup copies of Critical Software
Trusted Recovery
Vulnerability and Incident Management
Vulnerability Management

Cybersecurity Implementation Controls
Application Data Handling
Database Management System
Data Storage
In-Memory Data Handling
Data Transmission
Data Integrity
Authentication
Server Authentication
User Authentication
Standalone Code Identification
Server Application Authentication
Client Application Authentication
PKI Certificate Validation
Password Complexity and Maintenance
Authentication Credentials Protection
Use of Cryptography
Use of Symmetric Ciphers
Use of Message Authentication Codes and Hashes
Use of Digital Signature
User accounts
Account Rules
No Duplicate Accounts
Account Lockout
Application Sessions
Access Control
Input Validation
Validation of User Input
Web Encoding
Canonical Representation and Hidden Fields in Web Pages
Information Disclosure
Auditing
Notification and Audit Content
Audit Trails Protection
Configuring Management
Software Configuration Management
Testing
Test Plan and Procedures
Automated Tools
Deployment
Documentation
Auditing

Wireless Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls
Wireless LAN Risk Management
IEEE 802.11x Extensible Authentication Protocol
EAP-Transport Layer Security
Separation of Network
Virtual Private Network
User Authentication and Data Encryption Services
Wi-Fi Protected Access (WPA)
Access Point and Client Identification
RSN, WRAP and CCMP Protocols:
Wireless PAN Risk Management
Bluetooth Specification
Device-level Authentication:
Data encryption
Pairing/Bonding
Confidentiality, Integrity, Authentication, and Authorization
Security Models and Levels
Secure Simple Pairing
Key Management
Wireless PED Risk Management
Subscriber Identity Module (SIM)
Wireless Email

Comparison of the Implementation Controls discussed in class with GrubHub's existing Cybersecurity Implementation Controls.

Access Control Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation controls	**Status**
Identification credentials	
ID Card	Present
Password	Present
Digital signature	Present
PINs	Present
PKI certificate	Present
Photograph	Absent
Biometrics	Present
Personal authentication	
Password	Present
Private key	Present
Smart Card	Absent
Biometrics	Present
Access Control List	Present
Policies	Present
Privilege token database	Absent
Authorization	
Access Control List	Present
Security token	Present
Deny by default policy	Absent
Logical access control method	
Network architecture controls	Present
Remote network access	Present
Securing network ports	Present
Physical security for Secure Internet Protocol Router Network (SIPRNeT) Ports	Present
Logical network port security	Present
Port authentication using 802.1x	Present
Network access control (NAC) system	Present
Encryption	Present
PKI compliance requirements	Present
Password	Present
PINs	Present
Implementing Something you know	Present
DoD common access card as hardware token	Absent
Alternate login token	Absent
Physical access control methods	
Classified storage and handling	Present
Attended access	Present

CAC and defense biometric identification system for physical access control	Absent
Badges	Present
Memory card	Absent
Smart card	Present
PINs, combinations, and other forms of something you know	Present
Physical tokens	Present
Physical intrusion detection systems	Present
Biometric systems	
Fingerprint scanner	Present
Facial recognition	Present

Network Infrastructure Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation controls	**Status**
Enclave Protection	
Defense-in-depth	Present
Firewall	Present
Router	Present
IDS and IPS	Present
Encryption	Present
Enclave DMZ	Absent
Network Test Access Ports	Absent
Wireless Intrusion Detection System	Absent
Anti-Backdoor	Absent
VPN tunnel	Present
Firewalls	
Packet Filters	Present
Bastion Host	Absent
Stateful Inspection	Present
Deep Packet Inspection	Absent
Application Proxy Gateway	Present
Hybrid Technology Firewalls	Present
Proxy Servers	Present
Routers	
Router Table Integrity	Present
Secure Router Planes	Absent

Network Infrastructure Management Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation controls	**Status**
Ports, Protocols and Services	
Blocking Protocols at the enclave perimeter	Present
Blocking ICMPv4 Echo Request, Echo Reply and Redirect Packets	Present
Disable Traceroute	Present
Updating Access List Rules	Absent
IPv4 Address Filtering	Present
Unicast Reverse Path Forwarding	Absent
SYN Flood attacks	Present
Device Management	
Device and Asset Management	Present
Out-of-band Management	Present
In-band Management	Present
Device Monitoring	
SNMP	Present
Network Management Station	Present
Network Authentication, Authorization, and Accounting (Auditing)	
Authentication	Present
Authorization	Present
Accounting	Present
Auditing	Present
Router Password Protection	Present
NIDS – Network Intrusion Detection System	
External Network Intrusion Detection	Present
External Network Intrusion Detection	Present
Switches, VLANs	
Physical	Present
Virtual Local Area Networks	Present
VLAN Trunking	Absent
VLAN Port Security	Present
802.1x and Management Policy Server	Present
VPN	
Gateway-to-gateway:	Absent
Host-to-gateway:	Present
Host-to-host	Absent

Cybersecurity Implementation Controls	Status
Authentication – User accounts	
Application User	Present
Database Administrator	Present
Application Owner	Present
Application User Manager	Absent
Application Account	Absent
Database Auditor	Present
Database Operator	Absent
Passwords	Present
Certificates	Present
External Authentication	Partial
Credential Storage	Present
Authorization	
Role Based Access Control	Present
Renaming Default Accounts	Absent
Confidentiality	
Data Encryption	Present
Application Code Encryption	Present
Data File Encryption:	Present
Data Integrity	Present
Transaction Log	Present
Data Integrity	Present
Auditing	
Audit Logs Protection	Present
Audit Logs Retention	Present
Audit Reporting	Present
Replication and Federation	
Database	Present
Database Replication	Present
Clustering	
Database Clustering	Present
Least Privilege	Present
Protected Communication Path	Present
Backup and Recovery	
DBMS Backup	Present
Testing and Maintenance	Present
Authentication and Authorization	Present
OS Protections	
Dedicated Directories and Files	Present
Dedicated OS account	Absent
Updated Database Software	Present

Application Protections	
Audit Elevated Privileges	Present
Input Validation	Present
Authentication Methods	Present
Least Privilege Mechanism	Present
Network Protections	
Network Access	Present
Time and count limits	Partial
Encrypted and protected data across network	Present
Security Design and Configuration	
Procedural Review	Present
Configuration Specifications	Present
Compliance Testing	Present
Functional Architecture for IS Applications	Present
Non-repudiation	Present
Partitioning the application	Present
Ports, protocols, and services	Present
Configuration Management Process	Present
IA Documentation	Present
System Library Management Controls	Present
Security Structure Support Partitioning	Absent
System State Changes	Present
Software Baseline	Present
Group Identification and Authentication	Present
Individual Identification and Authentication	Present
Key Management	Present
Token and Certificate Standards	Present
Enclave and Computing environment	
Access for Need to Know	Present
Audit Record Content	Present
Audit Trail, Monitoring, Analysis and Reporting	Present
Changes to Data	Present
Encryption for Confidentiality	Present
Data Change Controls	Present
Interconnections among Systems and Enclaves	Present
Audit of Security Label Changes	Present
Logon	Present
Privileged Account Control	Present
Marketing and Labelling	Present
Production Code Change Controls	Present
Resource Control	Present
Audit Reduction and Report Generation	Absent
Security Configuration Compliance	Present
Software Development Change Controls	Present

Warning message	Present
Boundary Defense	Present
Remote Access for Privileged Functions	Partial
Business and Continuity	
Protection of Backup and Restoration Assets	Present
Data Backup Procedures	Present
Disaster and Recovery Planning	Present
Backup copies of Critical Software	Present
Trusted Recovery	Present
Vulnerability and Incident Management	
Vulnerability Management	Present

Applications Development Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls	Status
Application Data Handling	
Database Management System	Present
Data Storage	Present
In-Memory Data Handling	Present
Data Transmission	Present
Data Integrity	Present
Data Marking	Absent
Authentication	
Server Authentication	Present
User Authentication	Present
Signed Code Identification	Absent
Standalone Code Identification	Present
Server Application Authentication	Present
Client Application Authentication	Present
Combination Client Server Application Authentication	Absent
Application Component Authentication	Absent
PKI Certificate Validation	Present
Password Complexity and Maintenance	Present
Authentication Credentials Protection	Present
Use of Cryptography	
Use of Symmetric Ciphers	Present
Use of Message Authentication Codes and Hashes	Present
Use of Digital Signature	Present
User accounts	
Account Rules	Present
No Duplicate Accounts	Partially
Account Lockout	Present
Application Sessions	Present
Access Control	Present

Input Validation	
Validation of User Input	Present
Web Encoding	Present
Use of Static Analysis Tools	Absent
Canonical Representation and Hidden Fields in Web Pages	Present
Information Disclosure	Present
Race Conditions	Absent
Auditing	
Notification and Audit Content	Present
Audit Trails Protection	Present
Configuring Management	
Software Configuration Management	Present
Limit Unauthorized Individuals	Absent
Testing	
Test Plan and Procedures	Present
Automated Tools	Present
Deployment	
Documentation	Present
Auditing	Present

Wireless Security Risk Management Implementation Controls and Policies

Cybersecurity Implementation Controls	Status
Wireless LAN Risk Management	
IEEE 802.11x Extensible Authentication Protocol	Present
EAP-Transport Layer Security	Present
EAP-Tunneling Transport Layer Security	Absent
Protected Extensible Authentication Protocol (PEAP)	Absent
Separation of Network	Present
Virtual Private Network	Present
User Authentication and Data Encryption Services	Present
Wi-Fi Protected Access (WPA)	Present
Broadcasting Service Set Identifier (SSID)	Absent
Access Point and Client Identification	Present
RSN, WRAP and CCMP Protocols:	Present
Wireless PAN Risk Management	
Bluetooth Specification	Present
Device-level Authentication:	Present
Data encryption	Present
Pairing/Bonding	Present
Confidentiality, Integrity, Authentication, and Authorization	Present
Security Models and Levels	Present
Secure Simple Pairing	Present
Key Management	Present

Wireless WAN Risk Management	
Use of Cellular Digital Packet Data (CDPD)	Absent
Wireless RFID Risk Management	
RFID Tag Encryption	Absent
Wireless PED Risk Management	
Subscriber Identity Module (SIM)	Present
Wireless Email	Present
PDA Security	Absent

List of critical assets that exist at GrubHub

Asset	**Asset Type**	**Value ($)**
A1	Application	$1000000
A2	Information Systems	$750000
A3	Financial Resources	$250000
A4	System Design	$100000
A5	Reputation	Intangible

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

Vulnerabilities
Permanent tokens vulnerability
Unauthorized Access
Weak Authentication
Network based attacks
Impersonation – Brute force attack
Identity theft
Backdoor attack
Botnet attack
IP Spoofing
ARP Attack
DoS – Denial of Service
OS attacks

List of potential threats to GrubHub that could exploit vulnerabilities of critical assets

Threats
Lack of data integrity
lack of service (availability)
exposure of confidential information
Spoofing
Damage reputation
No service
Destroyed application
No confidentiality

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

Risks
Exposure of Confidential Information
Denial of Service – Users can’t access application
Unauthorized access due to weak authentication
Impersonation of privileged personnel
Attack Network system both application and website
Availability of Service
Man in the Middle attacks
Redirection of traffic
Application attack
Undetected attacks

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

- Strong policies on Wireless connection should be enforced to avoid sniffing.
- SSID should. Not be broadcasted.
- Software development life cycle should be carefully initialized, each step should be documented, tested, and ensured that policies used are following through the organization, nation, and global standards.
- Defaults accounts should be renamed to make it harder for attacker to use them in attacks.
- Sign in attempts should be limited and unresponsive logged sessions should be logged out. Though partially used, it should be applied to all applications.
- Application accounts should be created to ensure separation of data.
- Security structure support is already enforced but stored in the same network. It should be stored on separate networks.
- The current DMZ should be enforced with maximum security just like an Enclaved DMZ. This will ensure that advisory do not use the DMZ as a bridge to get to the Internal information stored in the access layer.
- With everything being remote, it is crucial to have some devices wireless. The organization currently have wired IDS and IPS devices that have few features which works fine and have not caused any issues so far. However, adding wireless IDS with more advanced features will make traffic monitoring process easier.
- Secure Router Planes should be configured properly to handles more traffic and re-direct traffic when overwhelmed instead of going through a DoD.
- Ensure ACL list and rules are updated regularly to avoid any unpredictable changes.
- The organization should install an Anti-unicast tool to ensure reverse path information are not leaked.
- Limiting Password retires: GrubHub should create a limit that a certain password can be used. Even with the presence of two-factor authentication, this vulnerability can be exploited successfully. The point of security in depth is to ensure that all layers of security are safe and hard to crack.
- The use of token database: instead of using a permanent token that is created when a user creates the account, GrubHub should enforce a policy where these tokens are changes periodically. Similar to the password to ensure access to their systems are secured and authenticated as needed.
- The use of CAC and defense biometric to add another layer of security in their authentication process. It is of no doubt that with the integration of mobile app and android and iPhone, this is now used by users when accessing the app. It will make GrubHub's systems more secure if the same measure is enforced when accessing their physical buildings.
- Limit unwanted traffic to their systems. This can be done by configuring the firewall appropriately.
- Use memory cards to add additional layer of security when authenticating users.
- Periodic monitoring of their systems should be enforced and analyzing data filtering the false positives.

List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience – Risk Response Strategy

- Backups should be made regularly and stored on different environments i.e., network.
- Prior to any change made, everything should be well documented, and a backup should be performed as a restore point.
- The use of encrypted backup incase the system gets compromised.
- Creating an incidence response plan which clearly state who is responsible for what when an incident occurs.
- Enforcing application and website to work on updated software version of user's devices to ensure transactions are done safely.
- Learning the root cause of the incident by investigation the logs.
- Limiting access to sensitive information. E.g., only necessary individuals can have access to the backdoor and when they need to access a one-time token should be used.
- Have users provide a secondary email for account recovery in case they lose their account to an advisory.
- The use of encrypted backup incase the system gets compromised.
- Creating an incidence response plan which clearly state who is responsible for what when an incident occurs.
- Users are educated on where to report and whom to contact when something suspicious happens to their accounts. Like requesting account deletion.
- Enforcing application and website to work on updated software version of user's devices to ensure transactions are done safely.
- Learning the root cause of the incident by investigation the logs.

Ranking of asset risk and Vulnerability risk for GrubHub access control, Network Infrastructure, Network Infrastructure Management, Database, Applications, and Wireless.

Domain	Top 5 Asset Risks	Top 5 Asset Vulnerabilities
Access Control	Exposure of Confidential Information	Unauthorized Access
	Denial of Service – Users can't access application	Weak Authentication
	Unauthorized access due to weak authentication	Network based attacks
	Impersonation of privileged personnel	Impersonation – Brute force attack
	Attack Network system both application and website	Identity theft
Network Infrastructure	Exposure of confidential Information	Network Attacks
	Availability of Service	Unauthorized access
	Man in the Middle attacks	Backdoor attack
	Redirection of traffic	Increases chances of penetration
	Application attack	Botnet attack
Network Infrastructure Management	Exposure of confidential Information	Network Attacks
	Availability of Service due to DoS	Unauthorized access
	Man in the Middle attacks	IP Spoofing
	Redirection of traffic	ARP Attack
	Application attack	DoS – Denial of Service
Database	No service	Network Attacks
	Loss of data integrity	Unauthorized access
	No confidentiality	Application layer attacks
	Destroyed application	OS attacks
	No service	DoS – Denial of Service
Applications	Exposure of confidential Information	Network Attacks
	Availability of Service due to DoS	Unauthorized access
	Undetected attacks	Application layer attacks
	Application attack	DoS – Denial of Service
	Exposure of confidential Information	Exposure of confidential Information
Wireless	Exposure of confidential Information	Network Attacks
	Availability of Service due to DoS	Unauthorized access
	Undetected attacks	Sniffing
	Identity can be spoofed	Exposure of confidential Information
	Exposure of confidential Information	DoS – Denial of Service

Top 5 Potential Vulnerabilities:	Top 5 Potential Risks:
Unauthorized Access	Exposure of Confidential Information
Application layer attacks	Denial of Service – Users can't access application
DoS – Denial of Service	Man in the Middle attacks
Network based attacks	Availability of Service
Impersonation – Brute force attack / Phishing	Attack Network system both application and website

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

- Strong policies on Wireless connection should be enforced to avoid sniffing.
- SSID should. Not be broadcasted.
- Software development life cycle should be carefully initialized, each step should be documented, tested, and ensured that policies used are following through the organization, nation, and global standards.
- Defaults accounts should be renamed to make it harder for attacker to use them in attacks.
- Sign in attempts should be limited and unresponsive logged sessions should be logged out. Though partially used, it should be applied to all applications.
- Application accounts should be created to ensure separation of data.
- Security structure support is already enforced but stored in the same network. It should be stored on separate networks.
- The current DMZ should be enforced with maximum security just like an Enclaved DMZ. This will ensure that advisory do not use the DMZ as a bridge to get to the Internal information stored in the access layer.
- With everything being remote, it is crucial to have some devices wireless. The organization currently have wired IDS and IPS devices that have few features which works fine and have not caused any issues so far. However, adding wireless IDS with more advanced features will make traffic monitoring process easier.
- Secure Router Planes should be configured properly to handles more traffic and re-direct traffic when overwhelmed instead of going through a DoD.
- Ensure ACL list and rules are updated regularly to avoid any unpredictable changes.
- The organization should install an Anti-unicast tool to ensure reverse path information are not leaked.

List of recommended Hardening Response controls and policies for critical assets that should be implemented to reduce asset risk impact and thus mitigate the identified risks and increase resilience – Risk Response Strategy

- Backups should be made regularly and stored on different environments i.e., network.
- Prior to any change made, everything should be well documented, and a backup should be performed as a restore point.
- The use of encrypted backup incase the system gets compromised.
- Creating an incidence response plan which clearly state who is responsible for what when an incident occurs.
- Enforcing application and website to work on updated software version of user's devices to ensure transactions are done safely.
- Learning the root cause of the incident by investigation the logs.
- Limiting access to sensitive information. E.g., only necessary individuals can have access to the backdoor and when they need to access a one-time token should be used.

Cybersecurity Workforce Risk Management Implementation:

List of Cybersecurity Specialty Areas that exist at GrubHub

Cybersecurity Specialty Areas
Risk Management (RSK)
Software Development (DEV)
Data Administration (DTA)
Network Services (NET)
Systems Administration (ADM)

List of Cybersecurity Work Roles that exist at GrubHub

Cybersecurity Work Roles
Authorizing Official/Designating Representative
Security Control Assessor
Software Developer
Database Administrator
Data Analyst
Network Operations Specialist
System Administrator

List of Cybersecurity Tasks that exist at GrubHub

Cybersecurity Tasks
Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
Establish acceptable limits for the software application, network, or system.
Manage Accreditation Packages (e.g., ISO/IEC 15026-2).
Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).
Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.
Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.
Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.
Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).

Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.
Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).
Verify and update security documentation reflecting the application/system security design features.
Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.
Assess the effectiveness of security controls.
Assess all the configuration management (change configuration/release management) processes.
Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.
Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.
Store, retrieve, and manipulate data for analysis of system capabilities and requirements.
Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.
Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.
Identify and leverage the enterprise-wide version control system while designing and developing secure applications.
Consult with customers about software system design and maintenance.
Direct software programming and development of documentation.
Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.
Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.
Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.
Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.

Develop software system testing and validation procedures, programming, and documentation.
Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.
Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.
Determine and document software patches or the extent of releases that would leave software vulnerable.
Analyze and plan for anticipated changes in data capacity requirements.
Maintain database management systems software.
Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.
Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.
Manage the compilation, cataloging, caching, distribution, and retrieval of data.
Monitor and maintain databases to ensure optimal performance.
Perform backup and recovery of databases to ensure data integrity.
Provide recommendations on new database technologies and architectures.
Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.
Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.
Maintain assured message delivery systems.
Implement data management standards, requirements, and specifications.
Implement data mining and data warehousing applications.
Install and configure database management systems and software.
Analyze and define data requirements and specifications.
Analyze and plan for anticipated changes in data capacity requirements.
Develop data standards, policies, and procedures.
Manage the compilation, cataloging, caching, distribution, and retrieval of data.
Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.
Provide recommendations on new database technologies and architectures.
Analyze data sources to provide actionable recommendations.
Assess the validity of source data and subsequent findings.
Collect metrics and trending data.

Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).
Develop and implement network backup and recovery procedures.
Diagnose network connectivity problem.
Implement new system design procedures, test procedures, and quality standards.
Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).
Install or replace network hubs, routers, and switches.
Integrate new systems into existing network architecture.
Monitor network capacity and performance.
Patch network vulnerabilities to ensure that information is safeguarded against outside parties.
Provide feedback on network requirements, including network architecture and infrastructure.
Test and maintain network infrastructure including software and hardware devices.
Conduct functional and connectivity testing to ensure continuing operability.
Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.
Develop and document systems administration standard operating procedures.
Maintain baseline system security according to organizational policies.
Manage accounts, network rights, and access to systems and equipment.
Plan, execute, and verify data redundancy and system recovery procedures.
Provide ongoing optimization and problem-solving support.
Install, update, and troubleshoot systems/servers.
Check system hardware availability, functionality, integrity, and efficiency.
Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.
Comply with organization systems administration standard operating procedures.
Implement and enforce local network usage policies and procedures.
Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.
Monitor and maintain system/server configuration.
Oversee installation, implementation, configuration, and support of system components.
Diagnose faulty system/server hardware.
Perform repairs on faulty system/server hardware.
Troubleshoot hardware/software interface and interoperability problems.

Comparison of the NCWF recommended Cybersecurity Specialty Areas with GrubHub existing Cybersecurity Specialty Areas

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

Comparison of the NCWF recommended Cybersecurity Work Roles and their NCWF recommended Cybersecurity Tasks with GrubHub existing Cybersecurity Work Roles and their existing Cybersecurity Tasks

Work Role	Tasks	Status
Authorizing Official/Designating Representative	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Present
	Establish acceptable limits for the software application, network, or system.	Present
	Manage Accreditation Packages (e.g., ISO/IEC 15026-2)	Present
Security Control Assessor	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Present
	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Present
	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Present
	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Present
	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	Present
	Establish acceptable limits for the software application, network, or system.	Absent
	Manage Accreditation Packages (e.g., ISO/IEC 15026-2).	Absent
	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Absent
	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Absent
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Verify and update security documentation reflecting the application/system security design features.	Present
	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Present
	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Absent
	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Absent
	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Absent

	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Absent
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Assess the effectiveness of security controls.	Absent
	Assess all the configuration management (change configuration/release management) processes.	Absent
	Manage and approve Accreditation Packages (e.g., ISO/IEC 15026-2).	Absent
	Plan and conduct security authorization reviews and assurance case development for initial installation of systems and networks.	Absent
	Review authorization and assurance documents to confirm that the level of risk is within acceptable limits for each software application, system, and network.	Absent
	Verify that application software/network/system security postures are implemented as stated, document deviations, and recommend required actions to correct those deviations.	Absent
	Develop security compliance processes and/or audits for external services (e.g., cloud service providers, data centers).	Present
	Establish acceptable limits for the software application, network, or system.	Present
Software Developer	Analyze information to determine, recommend, and plan the development of a new application or modification of an existing application.	Absent
	Analyze user needs and software requirements to determine feasibility of design within time and cost constraints.	Absent
	Apply coding and testing standards, apply security testing tools including "'fuzzing" static-analysis code scanning tools, and conduct code reviews.	Absent
	Apply secure code documentation.	Absent
	Capture security controls used during the requirements phase to integrate security within the process, to identify key security objectives, and to maximize software security while minimizing disruption to plans and schedules.	Present
	Compile and write documentation of program development and subsequent revisions, inserting comments in the coded instructions so others can understand the program.	Present
	Confer with systems analysts, engineers, programmers, and others to design application and to obtain information on project limitations and capabilities, performance requirements, and interfaces.	Present
	Consult with engineering staff to evaluate interface between hardware and software.	Present
	Correct errors by making appropriate changes and rechecking the program to ensure that desired results are produced.	Present
	Design, develop, and modify software systems, using scientific analysis and mathematical models to predict and measure outcome and consequences of design.	Present
	Develop secure code and error handling.	Present

	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Present
	Identify basic common coding flaws at a high level.	Present
	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.	Present
	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Present
	Perform integrated quality assurance testing for security functionality and resiliency attack.	Present
	Perform secure programming and identify potential flaws in codes to mitigate vulnerabilities.	Present
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Present
	Prepare detailed workflow charts and diagrams that describe input, output, and logical operation, and convert them into a series of instructions coded in a computer language.	Present
	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Present
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Present
	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Present
	Design countermeasures and mitigations against potential exploitations of programming language weaknesses and vulnerabilities in system and elements.	Present
	Identify and leverage the enterprise-wide version control system while designing and developing secure applications.	Present
	Consult with customers about software system design and maintenance.	Present
	Direct software programming and development of documentation.	Present
	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Present
	Enable applications with public keying by leveraging existing public key infrastructure (PKI) libraries and incorporating certificate management and encryption functionalities when appropriate.	Present
	Identify and leverage the enterprise-wide security services while designing and developing secure applications (e.g., Enterprise PKI, Federated Identity server, Enterprise Antivirus solution) when appropriate.	Present
	Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.	Present
	Develop software system testing and validation procedures, programming, and documentation.	Present

	Modify and maintain existing software to correct errors, to adapt it to new hardware, or to upgrade interfaces and improve performance.	Present
	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Present
	Determine and document software patches or the extent of releases that would leave software vulnerable.	Present
Secure Software Accessor	Develop threat model based on customer interviews and requirements.	Absent
	Consult with engineering staff to evaluate interface between hardware and software.	Absent
	Evaluate factors such as reporting formats required, cost constraints, and need for security restrictions to determine hardware configuration.	Absent
	Identify basic common coding flaws at a high level.	Absent
	Identify security implications and apply methodologies within centralized and decentralized environments across the enterprise's computer systems in software development.	Absent
	Identify security issues around steady state operation and management of software and incorporate security measures that must be taken when a product reaches its end of life.	Absent
	Perform integrated quality assurance testing for security functionality and resiliency attack.	Absent
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
	Address security implications in the software acceptance phase including completion criteria, risk acceptance and documentation, common criteria, and methods of independent testing.	Absent
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Absent
	Translate security requirements into application design elements including documenting the elements of the software attack surfaces, conducting threat modeling, and defining any specific security criteria.	Absent
	Perform penetration testing as required for new or updated applications.	Absent
	Consult with customers about software system design and maintenance.	Absent
	Direct software programming and development of documentation.	Absent
	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Absent
	Analyze and provide information to stakeholders that will support the development of security application or modification of an existing security application.	Absent
	Analyze security needs and software requirements to determine feasibility of design within time and cost constraints and security mandates.	Absent
	Conduct trial runs of programs and software applications to ensure that the desired information is produced and instructions and security levels are correct.	Absent
	Develop secure software testing and validation procedures.	Absent
	Develop system testing and validation procedures, programming, and documentation.	Absent

	Perform secure program testing, review, and/or assessment to identify potential flaws in codes and mitigate vulnerabilities.	Absent
	Determine and document software patches or the extent of releases that would leave software vulnerable.	Absent
Enterprise Architect	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Absent
	Employ secure configuration management processes.	Absent
	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Absent
	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Absent
	Provide advice on project costs, design concepts, or design changes.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Analyze candidate architectures, allocate security services, and select security mechanisms.	Absent
	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Absent
	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Absent
	Write detailed functional specifications that document the architecture development process.	Absent
	Analyze user needs and requirements to plan architecture.	Absent
	Capture and integrate essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Absent
	Develop enterprise architecture or system components required to meet user needs.	Absent
	Document and update as necessary all definition and architecture activities.	Absent
	Integrate results regarding the identification of gaps in security architecture.	Absent
	Plan implementation strategy to ensure that enterprise components can be integrated and aligned.	Absent
	Translate proposed capabilities into technical requirements.	Absent
	Document how the implementation of a new system or new interface between systems impacts the current and target environment including but not limited to security posture.	Absent
	Integrate key management functions as related to cyberspace.	Absent
Security Architect	Define and prioritize essential system capabilities or business functions required for partial or full system restoration after a catastrophic failure event.	Absent

	Define appropriate levels of system availability based on critical system functions and ensure that system requirements identify appropriate disaster recovery and continuity of operations requirements to include any appropriate fail-over/alternate site requirements, backup requirements, and material supportability requirements for system recover/restoration.	Absent
	Develop/integrate cybersecurity designs for systems and networks with multilevel security requirements or requirements for the processing of multiple classification levels of data primarily applicable to government organizations (e.g., UNCLASSIFIED, SECRET, and TOP SECRET).	Absent
	Document and address organization's information security, cybersecurity architecture, and systems security engineering requirements throughout the acquisition life cycle.	Absent
	Employ secure configuration management processes.	Absent
	Ensure that acquired or developed system(s) and architecture(s) are consistent with organization's cybersecurity architecture guidelines.	Absent
	Identify and prioritize critical business functions in collaboration with organizational stakeholders.	Absent
	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Absent
	Provide advice on project costs, design concepts, or design changes.	Absent
	Provide input on security requirements to be included in statements of work and other appropriate procurement documents.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Define and document how the implementation of a new system or new interfaces between systems impacts the security posture of the current environment.	Absent
	Analyze candidate architectures, allocate security services, and select security mechanisms.	Absent
	Develop a system security context, a preliminary system security Concept of Operations (CONOPS), and define baseline system security requirements in accordance with applicable cybersecurity requirements.	Absent
	Evaluate security architectures and designs to determine the adequacy of security design and architecture proposed or provided in response to requirements contained in acquisition documents.	Absent
	Write detailed functional specifications that document the architecture development process.	Absent
	Analyze user needs and requirements to plan architecture.	Absent
	Develop enterprise architecture or system components required to meet user needs.	Absent
	Document and update as necessary all definition and architecture activities.	Absent
	Determine the protection needs (i.e., security controls) for the information system(s) and network(s) and document appropriately.	Absent
	Translate proposed capabilities into technical requirements.	Absent
	Assess and design security management functions as related to cyberspace.	Absent

Research & Development Specialist	Review and validate data mining and data warehousing programs, processes, and requirements.	Absent
	Research current technology to understand capabilities of required system or network.	Absent
	Identify cyber capabilities strategies for custom hardware and software development based on mission requirements.	Absent
	Collaborate with stakeholders to identify and/or develop appropriate solutions technology.	Absent
	Design and develop new tools/technologies as related to cybersecurity.	Absent
	Evaluate network infrastructure vulnerabilities to enhance capabilities being developed.	Absent
	Follow software and systems engineering life cycle standards and processes.	Absent
	Troubleshoot prototype design and process issues throughout the product design, development, and pre-launch phases.	Absent
	Identify functional- and security-related features to find opportunities for new capability development to exploit or mitigate vulnerabilities.	Absent
	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Absent
	Develop data management capabilities (e.g., cloud-based, centralized cryptographic key management) to include support to the mobile workforce.	Absent
	Research and evaluate available technologies and standards to meet customer requirements.	Absent
Systems Requirements Planner	Conduct risk analysis, feasibility study, and/or trade-off analysis to develop, document, and refine functional requirements and specifications.	Absent
	Consult with customers to evaluate functional requirements.	Absent
	Coordinate with systems architects and developers, as needed, to provide oversight in the development of design solutions.	Absent
	Define project scope and objectives based on customer requirements.	Absent
	Develop and document requirements, capabilities, and constraints for design procedures and processes.	Absent
	Integrate and align information security and/or cybersecurity policies to ensure that system analysis meets security requirements.	Absent
	Oversee and make recommendations regarding configuration management.	Absent
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Absent
	Prepare use cases to justify the need for specific information technology (IT) solutions.	Absent
	Translate functional requirements into technical solutions.	Absent
	Develop and document supply chain risks for critical system elements, as appropriate.	Absent
	Develop and document User Experience (UX) requirements including information architecture and user interface requirements.	Absent
	Design and document quality standards.	Absent
	Document a system's purpose and preliminary system security concept of operations.	Absent
	Ensure that all systems components can be integrated and aligned (e.g., procedures, databases, policies, software, and hardware).	Absent

	Define baseline security requirements in accordance with applicable guidelines.	Absent
	Develop cost estimates for new or modified system(s).	Absent
	Manage the information technology (IT) planning process to ensure that developed solutions meet customer requirements.	Absent
System Testing and Evaluation Specialist	Determine level of assurance of developed capabilities based on test results.	Absent
	Develop test plans to address specifications and requirements.	Absent
	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Absent
	Make recommendations based on test results.	Absent
	Determine scope, infrastructure, resources, and data sample size to ensure system requirements are adequately demonstrated.	Absent
	Create auditable evidence of security measures.	Absent
	Validate specifications and requirements for testability.	Absent
	Analyze the results of software, hardware, or interoperability testing.	Absent
	Perform developmental testing on systems under development.	Absent
	Perform interoperability testing on systems exchanging electronic information with other systems.	Absent
	Perform operational testing.	Absent
	Test, evaluate, and verify hardware and/or software to determine compliance with defined specifications and requirements.	Absent
	Record and manage test data.	Absent
Information Systems Security Developer	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Absent
	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Absent
	Assess the effectiveness of cybersecurity measures utilized by system(s).	Absent
	Assess threats to and vulnerabilities of computer system(s) to develop a security risk profile.	Absent
	Build, test, and modify product prototypes using working models or theoretical models.	Absent
	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Absent
	Design and develop cybersecurity or cybersecurity-enabled products.	Absent
	Design hardware, operating systems, and software applications to adequately address cybersecurity requirements.	Absent
	Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Absent
	Develop and direct system testing and validation procedures and documentation.	Absent
	Develop detailed security design documentation for component and interface specifications to support system design and development.	Absent

	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Absent
	Develop risk mitigation strategies to resolve vulnerabilities and recommend security changes to system or system components as needed.	Absent
	Develop specific cybersecurity countermeasures and risk mitigation strategies for systems and/or applications.	Absent
	Identify components or elements, allocate security functions to those elements, and describe the relationships between the elements.	Absent
	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Absent
	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Absent
	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.	Absent
	Implement security designs for new or existing system(s).	Absent
	Incorporate cybersecurity vulnerability solutions into system designs (e.g., Cybersecurity Vulnerability Alerts).	Absent
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent
	Provide guidelines for implementing developed systems to customers or installation teams.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Absent
	Provide support to security/certification test and evaluation activities.	Absent
	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Absent
	Design and develop key management functions (as related to cybersecurity).	Absent
	Analyze user needs and requirements to plan and conduct system security development.	Absent
	Develop cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	Absent
	Ensure that security design and cybersecurity development activities are properly documented (providing a functional description of security implementation) and updated as necessary.	Absent

	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Absent
	Employ configuration management processes.	Absent
	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Absent
	Design, develop, integrate, and update system security measures that provide confidentiality, integrity, availability, authentication, and non-repudiation.	Absent
	Design to security requirements to ensure requirements are met for all systems and/or applications.	Absent
	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Absent
	Perform an information security risk assessment.	Absent
	Perform security reviews and identify security gaps in architecture.	Absent
	Provide input to implementation plans and standard operating procedures as they relate to information systems security.	Absent
	Trace system requirements to design components and perform gap analysis.	Absent
	Verify stability, interoperability, portability, and/or scalability of system architecture.	Absent
Systems Developer	Analyze design constraints, analyze trade-offs and detailed system and security design, and consider life cycle support.	Absent
	Build, test, and modify product prototypes using working models or theoretical models.	Absent
	Design and develop cybersecurity or cybersecurity-enabled products.	Absent
	Design or integrate appropriate data backup capabilities into overall system designs, and ensure that appropriate technical and procedural processes exist for secure system backups and protected storage of backup data.	Absent
	Develop and direct system testing and validation procedures and documentation.	Absent
	Develop architectures or system components consistent with technical specifications.	Absent
	Develop Disaster Recovery and Continuity of Operations plans for systems under development and ensure testing prior to systems entering a production environment.	Absent
	Identify and direct the remediation of technical problems encountered during testing and implementation of new systems (e.g., identify and find work-arounds for communication protocols that are not interoperable).	Absent
	Identify and prioritize essential system functions or sub-systems required to support essential capabilities or business functions for restoration or recovery after a system failure or during a system recovery event based on overall system requirements for continuity and availability.	Absent
	Identify, assess, and recommend cybersecurity or cybersecurity-enabled products for use within a system and ensure that recommended products are in compliance with organization's evaluation and validation requirements.	Absent
	Perform risk analysis (e.g., threat, vulnerability, and probability of occurrence) whenever an application or system undergoes a major change.	Absent

	Provide guidelines for implementing developed systems to customers or installation teams.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Store, retrieve, and manipulate data for analysis of system capabilities and requirements.	Absent
	Utilize models and simulations to analyze or predict system performance under different operating conditions.	Absent
	Implement and integrate system development life cycle (SDLC) methodologies (e.g., IBM Rational Unified Process) into development environment.	Absent
	Employ configuration management processes.	Absent
	Conduct a market analysis to identify, assess, and recommend commercial, Government off-the-shelf, and open source products for use within a system and ensure recommended products are in compliance with organization's evaluation and validation requirements.	Absent
	Design and develop system administration and management functionality for privileged access users.	Absent
	Design, implement, test, and evaluate secure interfaces between information systems, physical systems, and/or embedded technologies.	Absent
	Incorporates risk-driven systems maintenance updates process to address system deficiencies (periodically and out of cycle).	Absent
	Ensure that design and development activities are properly documented (providing a functional description of implementation) and updated as necessary.	Absent
	Design hardware, operating systems, and software applications to adequately address requirements.	Absent
	Design to security requirements to ensure requirements are met for all systems and/or applications.	Absent
	Develop detailed design documentation for component and interface specifications to support system design and development.	Absent
	Develop mitigation strategies to address cost, schedule, performance, and security risks.	Absent
	Identify components or elements, allocate comprehensive functional components to include security functions, and describe the relationships between the elements.	Absent
	Implement designs for new or existing system(s).	Absent
	Perform security reviews and identify security gaps in architecture.	Absent
	Provide input to implementation plans, standard operating procedures, maintenance documentation, and maintenance training materials	Absent
	Provide support to test and evaluation activities.	Absent
	Trace system requirements to design components and perform gap analysis.	Absent
	Verify stability, interoperability, portability, and/or scalability of system architecture.	Absent
	Analyze user needs and requirements to plan and conduct system development.	Absent

	Develop designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations.	Absent
	Collaborate on cybersecurity designs to meet specific operational needs and environmental factors (e.g., access controls, automated applications, networked operations, high integrity and availability requirements, multilevel security/processing of multiple classification levels, and processing Sensitive Compartmented Information).	Absent
Database Administrator	Analyze and plan for anticipated changes in data capacity requirements.	Present
	Maintain database management systems software.	Present
	Maintain directory replication services that enable information to replicate automatically from rear servers to forward units via optimized routing.	Present
	Maintain information exchanges through publish, subscribe, and alert functions that enable users to send and receive critical information as required.	Present
	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Present
	Monitor and maintain databases to ensure optimal performance.	Present
	Perform backup and recovery of databases to ensure data integrity.	Present
	Provide recommendations on new database technologies and architectures.	Present
	Performs configuration management, problem management, capacity management, and financial management for databases and data management systems.	Present
	Supports incident management, service-level management, change management, release management, continuity management, and availability management for databases and data management systems.	Present
	Maintain assured message delivery systems.	Present
	Implement data management standards, requirements, and specifications.	Present
	Implement data mining and data warehousing applications.	Present
	Install and configure database management systems and software.	Present
Data Analyst	Analyze and define data requirements and specifications.	Present
	Analyze and plan for anticipated changes in data capacity requirements.	Present
	Develop data standards, policies, and procedures.	Present
	Manage the compilation, cataloging, caching, distribution, and retrieval of data.	Present
	Provide a managed flow of relevant information (via web-based portals or other means) based on mission requirements.	Present
	Provide recommendations on new database technologies and architectures.	Present
	Analyze data sources to provide actionable recommendations.	Present
	Assess the validity of source data and subsequent findings.	Present
	Collect metrics and trending data.	Present
	Conduct hypothesis testing using statistical processes.	Absent
	Confer with systems analysts, engineers, programmers, and others to design application.	Absent
	Develop and facilitate data-gathering methods.	Absent
	Develop strategic insights from large data sets.	Absent
	Present technical information to technical and nontechnical audiences.	Absent

	Present data in creative formats.	Absent
	Program custom algorithms.	Absent
	Provide actionable recommendations to critical stakeholders based on data analysis and findings.	Absent
	Utilize technical documentation or resources to implement a new mathematical, data science, or computer science method.	Absent
	Effectively allocate storage capacity in the design of data management systems.	Absent
	Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	Absent
	Utilize different programming languages to write code, open files, read files, and write output to different files.	Absent
	Utilize open source language such as R and apply quantitative techniques (e.g., descriptive and inferential statistics, sampling, experimental design, parametric and non-parametric tests of difference, ordinary least squares regression, general line).	Absent
	Develop and implement data mining and data warehousing programs.	Absent
Knowledge Manager	Construct access paths to suites of information (e.g., link pages) to facilitate access by end-users.	Absent
	Develop an understanding of the needs and requirements of information end-users.	Absent
	Monitor and report the usage of knowledge management assets and resources.	Absent
	Plan and manage the delivery of knowledge management projects.	Absent
	Provide recommendations on data structures and databases that ensure correct and quality production of reports/management information.	Absent
	Lead efforts to promote the organization's use of knowledge management and information sharing.	Absent
	Manage the indexing/cataloguing, storage, and access of explicit organizational knowledge (e.g., hard copy documents, digital files).	Absent
	Design, build, implement, and maintain a knowledge management framework that provides end-users access to the organization’s intellectual capital.	Absent
	Promote knowledge sharing between information owners/users through an organization’s operational processes and systems.	Absent
Technical Support Specialist	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Absent
	Troubleshoot system hardware and software.	Absent
	Analyze incident data for emerging trends.	Absent
	Develop and deliver technical training to educate others or meet customer needs.	Absent
	Maintain incident tracking and solution database.	Absent
	Diagnose and resolve customer reported system incidents, problems, and events.	Absent

	Make recommendations based on trend analysis for enhancements to software and hardware solutions to enhance customer experience.	Absent
	Install and configure hardware, software, and peripheral equipment for system users in accordance with organizational standards.	Absent
	Administer accounts, network rights, and access to systems and equipment.	Absent
	Perform asset management/inventory of information technology (IT) resources.	Absent
	Monitor and report client-level computer system performance.	Absent
	Develop a trend analysis and impact report.	Absent
Network Operations Specialist	Configure and optimize network hubs, routers, and switches (e.g., higher-level protocols, tunneling).	Present
	Develop and implement network backup and recovery procedures.	Present
	Diagnose network connectivity problem.	Present
	Implement new system design procedures, test procedures, and quality standards.	Present
	Install and maintain network infrastructure device operating system software (e.g., IOS, firmware).	Present
	Install or replace network hubs, routers, and switches.	Present
	Integrate new systems into existing network architecture.	Present
	Monitor network capacity and performance.	Present
	Patch network vulnerabilities to ensure that information is safeguarded against outside parties.	Present
	Provide feedback on network requirements, including network architecture and infrastructure.	Present
	Test and maintain network infrastructure including software and hardware devices.	Present
System Administrator	Conduct functional and connectivity testing to ensure continuing operability.	Present
	Design group policies and access control lists to ensure compatibility with organizational standards, business rules, and needs.	Present
	Develop and document systems administration standard operating procedures.	Present
	Maintain baseline system security according to organizational policies.	Present
	Manage accounts, network rights, and access to systems and equipment.	Present
	Plan, execute, and verify data redundancy and system recovery procedures.	Present
	Provide ongoing optimization and problem-solving support.	Present
	Install, update, and troubleshoot systems/servers.	Present
	Check system hardware availability, functionality, integrity, and efficiency.	Present
	Conduct periodic system maintenance including cleaning (both physically and electronically), disk checks, routine reboots, data dumps, and testing.	Present
	Comply with organization systems administration standard operating procedures.	Present
	Implement and enforce local network usage policies and procedures.	Present
	Manage system/server resources including performance, capacity, availability, serviceability, and recoverability.	Present
	Monitor and maintain system/server configuration.	Present

	Oversee installation, implementation, configuration, and support of system components.	Present
	Diagnose faulty system/server hardware.	Present
	Perform repairs on faulty system/server hardware.	Present
	Troubleshoot hardware/software interface and interoperability problems.	Present
Systems Security Analyst	Apply security policies to applications that interface with one another, such as Business-to-Business (B2B) applications.	Absent
	Apply security policies to meet security objectives of the system.	Absent
	Apply service-oriented security architecture principles to meet organization's confidentiality, integrity, and availability requirements.	Absent
	Ensure all systems security operations and maintenance activities are properly documented and updated as necessary.	Absent
	Ensure that the application of security patches for commercial products integrated into system design meet the timelines dictated by the management authority for the intended operational environment.	Absent
	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Absent
	Implement specific cybersecurity countermeasures for systems and/or applications.	Absent
	Integrate automated capabilities for updating or patching system software where practical and develop processes and procedures for manual updating and patching of system software based on current and projected patch timeline requirements for the operational environment of the system.	Absent
	Perform cybersecurity testing of developed applications and/or systems.	Absent
	Perform security reviews, identify gaps in security architecture, and develop a security risk management plan.	Absent
	Plan and recommend modifications or adjustments based on exercise results or system environment.	Absent
	Properly document all systems security implementation, operations, and maintenance activities and update as necessary.	Absent
	Provide cybersecurity guidance to leadership.	Absent
	Provide input to the Risk Management Framework process activities and related documentation (e.g., system life-cycle support plans, concept of operations, operational procedures, and maintenance training materials).	Absent
	Verify and update security documentation reflecting the application/system security design features.	Absent
	Assess the effectiveness of security controls.	Absent
	Assess all the configuration management (change configuration/release management) processes.	Absent
	Develop procedures and test fail-over for system operations transfer to an alternate site based on system availability requirements.	Absent
	Analyze and report organizational security posture trends.	Absent
	Analyze and report system security posture trends.	Absent
	Assess adequate access controls based on principles of least privilege and need-to-know.	Absent
	Ensure the execution of disaster recovery and continuity of operations.	Absent

	Implement security measures to resolve vulnerabilities, mitigate risks, and recommend security changes to system or system components as needed.	Absent
	Implement system security measures in accordance with established procedures to ensure confidentiality, integrity, availability, authentication, and non-repudiation.	Absent
	Ensure the integration and implementation of Cross-Domain Solutions (CDS) in a secure environment.	Absent
	Mitigate/correct security deficiencies identified during security/certification testing and/or recommend risk acceptance for the appropriate senior leader or authorized representative.	Absent
	Assess and monitor cybersecurity related to system implementation and testing practices.	Absent
	Verify minimum security requirements are in place for all applications.	Absent
	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Absent
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Absent
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Absent
Cyber Legal Advisor	Advocate organization's official position in legal and legislative proceedings.	Absent
	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Absent
	Evaluate the effectiveness of laws, regulations, policies, standards, or procedures.	Absent
	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	Absent
	Conduct framing of pleadings to properly identify alleged violations of law, regulations, or policy/guidance.	Absent
	Develop guidelines for implementation.	Absent
	Provide legal analysis and decisions to inspectors general, privacy officers, oversight and compliance personnel regarding compliance with cybersecurity policies and relevant legal and regulatory requirements.	Absent
	Evaluate the impact of changes to laws, regulations, policies, standards, or procedures.	Absent
	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Absent
	Facilitate implementation of new or revised laws, regulations, executive orders, policies, standards, or procedures.	Absent
	Prepare legal and other relevant documents (e.g., depositions, briefs, affidavits, declarations, appeals, pleadings, discovery).	Absent
	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Absent

Privacy Officer/Privacy Compliance Manager	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Absent
	Conduct functional and connectivity testing to ensure continuing operability.	Absent
	Establish a risk management strategy for the organization that includes a determination of risk tolerance.	Absent
	Conduct Privacy Impact Assessments (PIAs) of the application's security design for the appropriate security controls, which protect the confidentiality and integrity of Personally Identifiable Information (PII).	Absent
	Develop and maintain strategic plans.	Absent
	Evaluate contracts to ensure compliance with funding, legal, and program requirements.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Absent
	Interpret and apply laws, regulations, policies, standards, or procedures to specific issues.	Absent
	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Absent
	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Absent
	Present technical information to technical and nontechnical audiences.	Absent
	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Absent
	Provide guidance on laws, regulations, policies, standards, or procedures to management, personnel, or clients.	Absent
	Work with the general counsel, external affairs and businesses to ensure both existing and new services comply with privacy and data security obligations.	Absent
	Work with legal counsel and management, key departments and committees to ensure the organization has and maintains appropriate privacy and confidentiality consent, authorization forms and information notices and materials reflecting current organization and legal practices and requirements.	Absent
	Coordinate with the appropriate regulating bodies to ensure that programs, policies and procedures involving civil rights, civil liberties and privacy considerations are addressed in an integrated and comprehensive manner.	Absent
	Liaise with regulatory and accrediting bodies.	Absent
	Work with external affairs to develop relationships with regulators and other government officials responsible for privacy and data security issues.	Absent
	Maintain current knowledge of applicable federal and state privacy laws and accreditation standards, and monitor advancements in information privacy technologies to ensure organizational adaptation and compliance.	Absent
	Ensure all processing and/or databases are registered with the local privacy/data protection authorities where required.	Absent
	Work with business teams and senior management to ensure awareness of "best practices" on privacy and data security issues.	Absent
	Work with organization senior management to establish an organization-wide Privacy Oversight Committee	Absent
	Serve in a leadership role for Privacy Oversight Committee activities	Absent

	Collaborate on cyber privacy and security policies and procedures	Absent
	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation	Absent
	Interface with Senior Management to develop strategic plans for the collection, use and sharing of information in a manner that maximizes its value while complying with applicable privacy regulations	Absent
	Provide strategic guidance to corporate officers regarding information resources and technology	Absent
	Assist the Security Officer with the development and implementation of an information infrastructure	Absent
	Coordinate with the Corporate Compliance Officer regarding procedures for documenting and reporting self-disclosures of any evidence of privacy violations.	Absent
	Work cooperatively with applicable organization units in overseeing consumer information access rights	Absent
	Serve as the information privacy liaison for users of technology systems	Absent
	Act as a liaison to the information systems department	Absent
	Develop privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations	Absent
	Oversee, direct, deliver or ensure delivery of initial privacy training and orientation to all employees, volunteers, contractors, alliances, business associates and other appropriate third parties	Absent
	Conduct on-going privacy training and awareness activities	Absent
	Work with external affairs to develop relationships with consumer organizations and other NGOs with an interest in privacy and data security issues—and to manage company participation in public events related to privacy and data security	Absent
	Work with organization administration, legal counsel and other related parties to represent the organization's information privacy interests with external parties, including government bodies, which undertake to adopt or amend privacy legislation, regulation or standard.	Absent
	Report on a periodic basis regarding the status of the privacy program to the Board, CEO or other responsible individual or committee	Absent
	Work with External Affairs to respond to press and other inquiries regarding concern over consumer and employee data	Absent
	Provide leadership for the organization's privacy program	Absent
	Direct and oversee privacy specialists and coordinate privacy and data security programs with senior executives globally to ensure consistency across the organization	Absent
	Ensure compliance with privacy practices and consistent application of sanctions for failure to comply with privacy policies for all individuals in the organization's workforce, extended workforce and for all business associates in cooperation with Human Resources, the information security officer, administration and legal counsel as applicable	Absent
	Develop appropriate sanctions for failure to comply with the corporate privacy policies and procedures	Absent

	Resolve allegations of noncompliance with the corporate privacy policies or notice of information practices	Absent
	Develop and coordinate a risk management and compliance framework for privacy	Absent
	Undertake a comprehensive review of the company's data and privacy projects and ensure that they are consistent with corporate privacy and data security goals and policies.	Absent
	Develop and manage enterprise-wide procedures to ensure the development of new products and services is consistent with company privacy policies and legal obligations	Absent
	Establish a process for receiving, documenting, tracking, investigating and acting on all complaints concerning the organization's privacy policies and procedures	Absent
	Establish with management and operations a mechanism to track access to protected health information, within the purview of the organization and as required by law and to allow qualified individuals to review or receive a report on such activity	Absent
	Provide leadership in the planning, design and evaluation of privacy and security related projects	Absent
	Establish an internal privacy audit program	Absent
	Periodically revise the privacy program considering changes in laws, regulatory or company policy	Absent
	Provide development guidance and assist in the identification, implementation and maintenance of organization information privacy policies and procedures in coordination with organization management and administration and legal counsel	Absent
	Assure that the use of technologies maintains, and does not erode, privacy protections on use, collection and disclosure of personal information	Absent
	Monitor systems development and operations for security and privacy compliance	Absent
	Conduct privacy impact assessments of proposed rules on the privacy of personal information, including the type of personal information collected and the number of people affected	Absent
	Conduct periodic information privacy impact assessments and ongoing compliance monitoring activities in coordination with the organization's other compliance and operational assessment functions	Absent
	Review all system-related information security plans to ensure alignment between security and privacy practices	Absent
	Work with all organization personnel involved with any aspect of release of protected information to ensure coordination with the organization's policies, procedures and legal requirements	Absent
	Account for and administer individual requests for release or disclosure of personal and/or protected information	Absent
	Develop and manage procedures for vetting and auditing vendors for compliance with the privacy and data security policies and legal requirements	Absent

	Participate in the implementation and ongoing compliance monitoring of all trading partner and business associate agreements, to ensure all privacy concerns, requirements and responsibilities are addressed	Absent
	Act as, or work with, counsel relating to business partner contracts	Absent
	Mitigate effects of a use or disclosure of personal information by employees or business partners	Absent
	Develop and apply corrective action procedures	Absent
	Administer action on all complaints concerning the organization's privacy policies and procedures in coordination and collaboration with other similar functions and, when necessary, legal counsel	Absent
	Support the organization's privacy compliance program, working closely with the Privacy Officer, Chief Information Security Officer, and other business leaders to ensure compliance with federal and state privacy laws and regulations	Absent
	Identify and correct potential company compliance gaps and/or areas of risk to ensure full compliance with privacy regulations	Absent
	Manage privacy incidents and breaches in conjunction with the Privacy Officer, Chief Information Security Officer, legal counsel and the business units	Absent
	Coordinate with the Chief Information Security Officer to ensure alignment between security and privacy practices	Absent
	Establish, implement and maintains organization-wide policies and procedures to comply with privacy regulations	Absent
	Ensure that the company maintains appropriate privacy and confidentiality notices, consent and authorization forms, and materials	Absent
Cyber Instructional Curriculum Developer	Support the design and execution of exercise scenarios.	Absent
	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Absent
	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Absent
	Research current technology to understand capabilities of required system or network.	Absent
	Assess effectiveness and efficiency of instruction according to ease of instructional technology use and student learning, knowledge transfer, and satisfaction.	Absent
	Conduct learning needs assessments and identify requirements.	Absent
	Create interactive learning exercises to create an effective learning environment.	Absent
	Develop or assist in the development of training policies and protocols for cyber training.	Absent
	Develop the goals and objectives for cyber curriculum.	Absent
	Plan instructional strategies such as lectures, demonstrations, interactive exercises, multimedia presentations, video courses, web-based courses for most effective learning environment in conjunction with educators and trainers.	Absent
	Correlate training and learning to business or mission requirements.	Absent

	Create training courses tailored to the audience and physical environment.	Absent
	Design training curriculum and course content based on requirements.	Absent
	Participate in development of training curriculum and course content.	Absent
	Conduct periodic reviews/revisions of course content for accuracy, completeness alignment, and currency (e.g., course content documents, lesson plans, student texts, examinations, schedules of instruction, and course descriptions).	Absent
	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Absent
	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.	Absent
Cyber Instructor	Conduct interactive training exercises to create an effective learning environment.	Absent
	Develop new or identify existing awareness and training materials that are appropriate for intended audiences.	Absent
	Evaluate the effectiveness and comprehensiveness of existing training programs.	Absent
	Review training documentation (e.g., Course Content Documents [CCD], lesson plans, student texts, examinations, Schedules of Instruction [SOI], and course descriptions).	Absent
	Support the design and execution of exercise scenarios.	Absent
	Write instructional materials (e.g., standard operating procedures, production manual) to provide detailed guidance to relevant portion of the workforce.	Absent
	Develop or assist in the development of computer based training modules or classes.	Absent
	Develop or assist in the development of course assignments.	Absent
	Develop or assist in the development of course evaluations.	Absent
	Develop or assist in the development of grading and proficiency standards.	Absent
	Assist in the development of individual/collective development, training, and/or remediation plans.	Absent
	Develop or assist in the development of learning objectives and goals.	Absent
	Develop or assist in the development of on-the-job training materials or programs.	Absent
	Develop or assist in the development of written tests for measuring and assessing learner proficiency.	Absent
	Conduct learning needs assessments and identify requirements.	Absent
	Develop or assist in the development of training policies and protocols for cyber training.	Absent
	Develop the goals and objectives for cyber curriculum.	Absent
	Present technical information to technical and nontechnical audiences.	Absent
	Present data in creative formats.	Absent
	Write and publish after action reviews.	Absent
	Deliver training courses tailored to the audience and physical/virtual environments.	Absent

	Apply concepts, procedures, software, equipment, and/or technology applications to students.	Absent
	Design training curriculum and course content based on requirements.	Absent
	Participate in development of training curriculum and course content.	Absent
	Ensure that training meets the goals and objectives for cybersecurity training, education, or awareness.	Absent
	Plan and coordinate the delivery of classroom techniques and formats (e.g., lectures, demonstrations, interactive exercises, multimedia presentations) for the most effective learning environment.	Absent
	Plan non-classroom educational techniques and formats (e.g., video courses, mentoring, web-based courses).	Absent
	Recommend revisions to curriculum and course content based on feedback from previous training sessions.	Absent
	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Absent
	Develop or assist with the development of privacy training materials and other communications to increase employee understanding of company privacy policies, data handling practices and procedures and legal obligations.	Absent
Information Systems Security Manager	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Absent
	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Absent
	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Absent
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Absent
	Advise appropriate senior leadership or Authorizing Official of changes affecting the organization's cybersecurity posture.	Absent
	Collect and maintain data needed to meet system cybersecurity reporting.	Absent
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Absent
	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Absent
	Ensure that security improvement actions are evaluated, validated, and implemented as required.	Absent
	Ensure that cybersecurity inspections, tests, and reviews are coordinated for the network environment.	Absent
	Ensure that cybersecurity requirements are integrated into the continuity planning for that system and/or organization(s).	Absent
	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with organization-level cybersecurity architecture.	Absent
	Establish overall enterprise information security architecture (EISA) with the organization’s overall security strategy.	Absent

	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Absent
	Identify alternative information security strategies to address organizational security objective.	Absent
	Identify information technology (IT) security program implications of new technologies or technology upgrades.	Absent
	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.	Absent
	Interpret and/or approve security requirements relative to the capabilities of new information technologies.	Absent
	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enterprise's cybersecurity program.	Absent
	Lead and align information technology (IT) security priorities with the security strategy.	Absent
	Lead and oversee information security budget, staffing, and contracting.	Absent
	Manage the monitoring of information security data sources to maintain organizational situational awareness.	Absent
	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Absent
	Manage threat or target analysis of cyber defense information and production of threat information within the enterprise.	Absent
	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	Absent
	Oversee the information security training and awareness program.	Absent
	Participate in an information security risk assessment during the Security Assessment and Authorization process.	Absent
	Participate in the development or modification of the computer environment cybersecurity program plans and requirements.	Absent
	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.	Absent
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Absent
	Provide leadership and direction to information technology (IT) personnel by ensuring that cybersecurity awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.	Absent
	Provide system-related input on cybersecurity requirements to be included in statements of work and other appropriate procurement documents.	Absent
	Provide technical documents, incident reports, findings from computer examinations, summaries, and other situational awareness information to higher headquarters.	Absent
	Recognize a possible security violation and take appropriate action to report the incident, as required.	Absent

	Recommend resource allocations required to securely operate and maintain an organization's cybersecurity requirements.	Absent
	Recommend policy and coordinate review and approval.	Absent
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
	Track audit findings and recommendations to ensure that appropriate mitigation actions are taken.	Absent
	Use federal and organization-specific published documents to manage operations of their computing environment system(s).	Absent
	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Absent
	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Absent
	Participate in Risk Governance process to provide security risks, mitigations, and input on other technical risk.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.	Absent
	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Absent
	Assure successful implementation and functionality of security requirements and appropriate information technology (IT) policies and procedures that are consistent with the organization's mission and goals.	Absent
	Support necessary compliance activities (e.g., ensure that system security configuration guidelines are followed, compliance monitoring occurs).	Absent
	Participate in the acquisition process as necessary, following appropriate supply chain risk management practices.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Continuously validate the organization against policies/guidelines/procedures/regulations/laws to ensure compliance.	Absent
	Forecast ongoing service demands and ensure that security assumptions are reviewed as necessary.	Absent
	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Absent
Communications Security (COMSEC) Manager	Advise senior management (e.g., Chief Information Officer [CIO]) on risk levels and security posture.	Absent
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Absent
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Absent
	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Absent
	Ensure that security improvement actions are evaluated, validated, and implemented as required.	Absent

	Establish overall enterprise information security architecture (EISA) with the organization's overall security strategy.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Absent
	Recognize a possible security violation and take appropriate action to report the incident, as required.	Absent
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
Cyber Workforce Developer and Manager	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Absent
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Absent
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Absent
	Collaborate with stakeholders to establish the enterprise continuity of operations program, strategy, and mission assurance.	Absent
	Develop policy, programs, and guidelines for implementation.	Absent
	Establish and maintain communication channels with stakeholders.	Absent
	Evaluate cost/benefit, economic, and risk analysis in decision-making process.	Absent
	Identify organizational policy stakeholders.	Absent
	Review existing and proposed policies with stakeholders.	Absent
	Serve on agency and interagency policy boards.	Absent
	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Absent
	Conduct learning needs assessments and identify requirements.	Absent
	Coordinate with internal and external subject matter experts to ensure existing qualification standards reflect organizational functional requirements and meet industry standards.	Absent
	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Absent
	Develop and implement standardized position descriptions based on established cyber work roles.	Absent
	Develop and review recruiting, hiring, and retention procedures in accordance with current HR policies.	Absent
	Develop cyber career field classification structure to include establishing career field entry requirements and other nomenclature such as codes and identifiers.	Absent
	Develop or assist in the development of training policies and protocols for cyber training.	Absent
	Ensure that cyber career fields are managed in accordance with organizational HR policies and directives.	Absent
	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	Absent

	Establish and collect metrics to monitor and validate cyber workforce readiness including analysis of cyber workforce data to assess the status of positions identified, filled, and filled with qualified personnel.	Absent
	Establish and oversee waiver processes for cyber career field entry and training qualification requirements.	
	Establish cyber career paths to allow career progression, deliberate development, and growth within and between cyber career fields.	
	Establish manpower, personnel, and qualification data element standards to support cyber workforce management and reporting requirements.	
	Establish, resource, implement, and assess cyber workforce management programs in accordance with organizational requirements.	
	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	
	Review and apply cyber career field qualification standards.	
	Review and apply organizational policies related to or influencing the cyber workforce.	
	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	
	Support integration of qualified cyber workforce personnel into information systems life cycle development processes.	
	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	
	Analyze organizational cyber policy.	
	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	
	Correlate training and learning to business or mission requirements.	
	Define and integrate current and future mission environments.	
	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.	
	Draft, staff, and publish cyber policy.	
	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	
	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	
	Seek consensus on proposed policy changes from stakeholders.	
	Provide policy guidance to cyber management, staff, and users.	
	Review, conduct, or participate in audits of cyber programs and projects.	Absent
	Serve as an internal consultant and advisor in own area of expertise (e.g., technical, copyright, print media, electronic media).	Absent
	Support the CIO in the formulation of cyber-related policies.	Absent
	Review and approve a supply chain security/risk management policy.	Absent
Cyber Policy and Strategy Planner	Develop policy, programs, and guidelines for implementation.	Absent
	Establish and maintain communication channels with stakeholders.	Absent
	Review existing and proposed policies with stakeholders.	Absent
	Serve on agency and interagency policy boards.	Absent

	Advocate for adequate funding for cyber training resources, to include both internal and industry-provided courses, instructors, and related materials.	Absent
	Ensure that cyber workforce management policies and processes comply with legal and organizational requirements regarding equal opportunity, diversity, and fair hiring/employment practices.	Absent
	Promote awareness of cyber policy and strategy as appropriate among management and ensure sound principles are reflected in the organization's mission, vision, and goals.	Absent
	Review/Assess cyber workforce effectiveness to adjust skill and/or qualification standards.	Absent
	Interpret and apply applicable laws, statutes, and regulatory documents and integrate into policy.	Absent
	Analyze organizational cyber policy.	Absent
	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Absent
	Define and integrate current and future mission environments.	Absent
	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.	Absent
	Draft, staff, and publish cyber policy.	Absent
	Monitor the rigorous application of cyber policies, principles, and practices in the delivery of planning and management services.	Absent
	Seek consensus on proposed policy changes from stakeholders.	Absent
	Provide policy guidance to cyber management, staff, and users.	Absent
	Review, conduct, or participate in audits of cyber programs and projects.	Absent
	Support the CIO in the formulation of cyber-related policies.	Absent
Executive Cyber Leadership	Acquire and manage the necessary resources, including leadership support, financial resources, and key security personnel, to support information technology (IT) security goals and objectives and reduce overall organizational risk.	Absent
	Acquire necessary resources, including financial resources, to conduct an effective enterprise continuity of operations program.	Absent
	Advise senior management (e.g., CIO) on cost/benefit analysis of information security programs, policies, processes, systems, and elements.	Absent
	Advocate organization's official position in legal and legislative proceedings.	Absent
	Communicate the value of information technology (IT) security throughout all levels of the organization stakeholders.	Absent
	Develop and maintain strategic plans.	Absent
	Interface with external organizations (e.g., public affairs, law enforcement, Command or Component Inspector General) to ensure appropriate and accurate dissemination of incident and other Computer Network Defense information.	Absent
	Lead and align information technology (IT) security priorities with the security strategy.	Absent
	Lead and oversee information security budget, staffing, and contracting.	Absent
	Manage the publishing of Computer Network Defense guidance (e.g., TCNOs, Concept of Operations, Net Analyst Reports, NTSM, MTOs) for the enterprise constituency.	Absent

	Monitor and evaluate the effectiveness of the enterprise's cybersecurity safeguards to ensure that they provide the intended level of protection.	Absent
	Recommend policy and coordinate review and approval.	Absent
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
	Supervise or manage protective or corrective measures when a cybersecurity incident or vulnerability is discovered.	Absent
	Promote awareness of security issues among management and ensure sound security principles are reflected in the organization's vision and goals.	Absent
	Oversee policy standards and implementation strategies to ensure procedures and guidelines comply with cybersecurity policies.	Absent
	Identify security requirements specific to an information technology (IT) system in all phases of the system life cycle.	Absent
	Ensure that plans of actions and milestones or remediation plans are in place for vulnerabilities identified during risk assessments, audits, inspections, etc.	Absent
	Define and/or implement policies and procedures to ensure protection of critical infrastructure as appropriate.	Absent
	Supervise and assign work to programmers, designers, technologists and technicians, and other engineering and scientific personnel.	Absent
	Coordinate with organizational manpower stakeholders to ensure appropriate allocation and distribution of human capital assets.	Absent
	Assess policy needs and collaborate with stakeholders to develop policies to govern cyber activities.	Absent
	Design/integrate a cyber strategy that outlines the vision, mission, and goals that align with the organization’s strategic plan.	Absent
	Perform an information security risk assessment.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
	Collaborate on cyber privacy and security policies and procedures	Absent
	Collaborate with cybersecurity personnel on the security risk assessment process to address privacy compliance and risk mitigation	Absent
	Appoint and guide a team of IT security experts.	Absent
	Collaborate with key stakeholders to establish a cybersecurity risk management program.	Absent
Program Manager	Develop and maintain strategic plans.	Absent
	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Absent
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Absent
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent

	Develop and document supply chain risks for critical system elements, as appropriate.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Develop contract language to ensure supply chain, system, network, and operational security are met.	Absent
	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Absent
	Coordinate and manage the overall service provided to a customer end-to-end.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Absent
	Participate in the acquisition process as necessary.	Absent
	Conduct import/export reviews for acquiring systems and software.	Absent
	Develop supply chain, system, network, performance, and cybersecurity requirements.	Absent
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent
	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Absent
	Lead and oversee budget, staffing, and contracting.	Absent
	Draft and publish supply chain security and risk management documents.	Absent
IT Project Manager	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Absent
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Absent
	Provide advice on project costs, design concepts, or design changes.	Absent
	Provide enterprise cybersecurity and supply chain risk management guidance for development of the Continuity of Operations Plans.	Absent
	Provide ongoing optimization and problem-solving support.	Absent
	Provide recommendations for possible improvements and upgrades.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Develop and document supply chain risks for critical system elements, as appropriate.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent

	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Absent
	Coordinate and manage the overall service provided to a customer end-to-end.	Absent
	Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Manage the internal relationship with information technology (IT) process owners supporting the service, assisting with the definition and agreement of Operating Level Agreements (OLAs).	Absent
	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Absent
	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Absent
	Participate in the acquisition process as necessary.	Absent
	Conduct import/export reviews for acquiring systems and software.	Absent
	Develop supply chain, system, network, performance, and cybersecurity requirements.	Absent
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent
	Identify and address cyber workforce planning and management issues (e.g. recruitment, retention, and training).	Absent
	Lead and oversee budget, staffing, and contracting.	Absent
	Draft and publish supply chain security and risk management documents.	Absent
Product Support Manager	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Absent
	Perform needs analysis to determine opportunities for new and improved business process solutions.	Absent
	Provide advice on project costs, design concepts, or design changes.	Absent
	Provide input to implementation plans and standard operating procedures.	Absent
	Provide ongoing optimization and problem-solving support.	Absent
	Provide recommendations for possible improvements and upgrades.	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Develop and document supply chain risks for critical system elements, as appropriate.	Absent

	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Develop contract language to ensure supply chain, system, network, and operational security are met.	Absent
	Act as a primary stakeholder in the underlying information technology (IT) operational processes and functions that support the service, provide direction and monitor all significant activities so the service is delivered successfully.	Absent
	Coordinate and manage the overall service provided to a customer end-to-end.	Absent
	Ensure that appropriate Service-Level Agreements (SLAs) and underpinning contracts have been defined that clearly set out for the customer a description of the service and the measures for monitoring the service.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Absent
	Work with other service managers and product owners to balance and prioritize services to meet overall customer requirements, constraints, and objectives.	Absent
	Conduct import/export reviews for acquiring systems and software.	Absent
	Develop supply chain, system, network, performance, and cybersecurity requirements.	Absent
	Lead and oversee budget, staffing, and contracting.	Absent
	Provide enterprise cybersecurity and supply chain risk management guidance.	Absent
	Draft and publish supply chain security and risk management documents.	Absent
	Apply cybersecurity functions (e.g., encryption, access control, and identity management) to reduce exploitation opportunities.	Absent
IT Investment/Portfolio Manager	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Ensure that all acquisitions, procurements, and outsourcing efforts address information security requirements consistent with organization goals.	Absent
	Develop contract language to ensure supply chain, system, network, and operational security are met.	Absent
	Gather feedback on customer satisfaction and internal service performance to foster continual improvement.	Absent
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent
	Lead and oversee budget, staffing, and contracting.	Absent
	Draft and publish supply chain security and risk management documents.	Absent
IT Program Auditor	Develop methods to monitor and measure risk, compliance, and assurance efforts.	Absent
	Provide ongoing optimization and problem-solving support.	Absent
	Provide recommendations for possible improvements and upgrades.	Absent

	Review or conduct audits of information technology (IT) programs and projects.	Absent
	Evaluate the effectiveness of procurement function in addressing information security requirements and supply chain risks through procurement activities and recommend improvements.	Absent
	Review service performance reports identifying any significant issues and variances, initiating, where necessary, corrective actions and ensuring that all outstanding issues are followed up.	Absent
	Conduct import/export reviews for acquiring systems and software.	Absent
	Ensure that supply chain, system, network, performance, and cybersecurity requirements are included in contract language and delivered.	Absent
Cyber Defense Analyst	Develop content for cyber defense tools.	Absent
	Characterize and analyze network traffic to identify anomalous activity and potential threats to network resources.	Absent
	Coordinate with enterprise-wide cyber defense staff to validate network alerts.	Absent
	Ensure that cybersecurity-enabled products or other compensating security control technologies reduce identified risk to an acceptable level.	Absent
	Document and escalate incidents (including event's history, status, and potential impact for further action) that may cause ongoing and immediate impact to the environment.	Absent
	Perform cyber defense trend analysis and reporting.	Absent
	Perform event correlation using information gathered from a variety of sources within the enterprise to gain situational awareness and determine the effectiveness of an observed attack.	Absent
	Perform security reviews and identify security gaps in security architecture resulting in recommendations for inclusion in the risk mitigation strategy.	Absent
	Plan and recommend modifications or adjustments based on exercise results or system environment.	Absent
	Provide daily summary reports of network events and activity relevant to cyber defense practices.	Absent
	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Absent
	Provide timely detection, identification, and alerting of possible attacks/intrusions, anomalous activities, and misuse activities and distinguish these incidents and events from benign activities.	Absent
	Use cyber defense tools for continual monitoring and analysis of system activity to identify malicious activity.	Absent
	Analyze identified malicious activity to determine weaknesses exploited, exploitation methods, effects on system and information.	Absent
	Determine tactics, techniques, and procedures (TTPs) for intrusion sets.	Absent
	Examine network topologies to understand data flows through the network.	Absent
	Recommend computing environment vulnerability corrections.	Absent
	Identify and analyze anomalies in network traffic using metadata.	Absent
	Conduct research, analysis, and correlation across a wide variety of all source data sets (indications and warnings).	Absent

	Validate intrusion detection system (IDS) alerts against network traffic using packet analysis tools.	Absent
	Isolate and remove malware.	Absent
	Identify applications and operating systems of a network device based on network traffic.	Absent
	Reconstruct a malicious attack or activity based off network traffic.	Absent
	Identify network mapping and operating system (OS) fingerprinting activities.	Absent
	Assist in the construction of signatures which can be implemented on cyber defense network tools in response to new or observed threats within the network environment or enclave.	Absent
	Notify designated managers, cyber incident responders, and cybersecurity service provider team members of suspected cyber incidents and articulate the event's history, status, and potential impact for further action in accordance with the organization's cyber incident response plan.	Absent
	Analyze and report organizational security posture trends.	Absent
	Analyze and report system security posture trends.	Absent
	Assess adequate access controls based on principles of least privilege and need-to-know.	Absent
	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.	Absent
	Assess and monitor cybersecurity related to system implementation and testing practices.	Absent
	Provides cybersecurity recommendations to leadership based on significant threats and vulnerabilities.	Absent
	Work with stakeholders to resolve computer security incidents and vulnerability compliance.	Absent
	Provide advice and input for Disaster Recovery, Contingency, and Continuity of Operations Plans.	Absent
Cyber Defense Infrastructure Support Specialist	Coordinate with Cyber Defense Analysts to manage and administer the updating of rules and signatures (e.g., intrusion detection/protection systems, antivirus, and content blacklists) for specialized cyber defense applications.	Absent
	Perform system administration on specialized cyber defense applications and systems (e.g., antivirus, audit and remediation) or Virtual Private Network (VPN) devices, to include installation, configuration, maintenance, backup, and restoration.	Absent
	Assist in identifying, prioritizing, and coordinating the protection of critical cyber defense infrastructure and key resources.	Absent
	Build, install, configure, and test dedicated cyber defense hardware.	Absent
	Assist in assessing the impact of implementing and sustaining a dedicated cyber defense infrastructure.	Absent
	Administer test bed(s), and test and evaluate applications, hardware infrastructure, rules/signatures, access controls, and configurations of platforms managed by service provider(s).	Absent

	Create, edit, and manage network access control lists on specialized cyber defense systems (e.g., firewalls and intrusion prevention systems).	Absent
	Identify potential conflicts with implementation of any cyber defense tools (e.g., tool and signature testing and optimization).	Absent
	Implement Risk Management Framework (RMF)/Security Assessment and Authorization (SA&A) requirements for dedicated cyber defense systems within the enterprise, and document and maintain records for them.	Absent
Cyber Defense Incident Responder	Coordinate and provide expert technical support to enterprise-wide cyber defense technicians to resolve cyber defense incidents.	Absent
	Correlate incident data to identify specific vulnerabilities and make recommendations that enable expeditious remediation.	Absent
	Perform analysis of log files from a variety of sources (e.g., individual host logs, network traffic logs, firewall logs, and intrusion detection system [IDS] logs) to identify possible threats to network security.	Absent
	Perform cyber defense incident triage, to include determining scope, urgency, and potential impact, identifying the specific vulnerability, and making recommendations that enable expeditious remediation.	Absent
	Perform cyber defense trend analysis and reporting.	Absent
	Perform initial, forensically sound collection of images and inspect to discern possible mitigation/remediation on enterprise systems.	Absent
	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	Absent
	Receive and analyze network alerts from various sources within the enterprise and determine possible causes of such alerts.	Absent
	Track and document cyber defense incidents from initial detection through final resolution.	Absent
	Write and publish cyber defense techniques, guidance, and reports on incident findings to appropriate constituencies.	Absent
	Employ approved defense-in-depth principles and practices (e.g., defense-in-multiple places, layered defenses, security robustness).	Absent
	Collect intrusion artifacts (e.g., source code, malware, Trojans) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Absent
	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Absent
	Coordinate with intelligence analysts to correlate threat assessment data.	Absent
	Write and publish after action reviews.	Absent
	Monitor external data sources (e.g., cyber defense vendor sites, Computer Emergency Response Teams, Security Focus) to maintain currency of cyber defense threat condition and determine which security issues may have an impact on the enterprise.	Absent
	Coordinate incident response functions.	Absent
Vulnerability Assessment Analyst	Analyze organization's cyber defense policies and configurations and evaluate compliance with regulations and organizational directives.	Absent
	Conduct and/or support authorized penetration testing on enterprise network assets.	Absent

	Maintain deployable cyber defense audit toolkit (e.g., specialized cyber defense software and hardware) to support cyber defense audit missions.	Absent
	Maintain knowledge of applicable cyber defense policies, regulations, and compliance documents specifically related to cyber defense auditing.	Absent
	Prepare audit reports that identify technical and procedural findings, and provide recommended remediation strategies/solutions.	Absent
	Conduct required reviews as appropriate within environment (e.g., Technical Surveillance, Countermeasure Reviews [TSCM], TEMPEST countermeasure reviews).	Absent
	Perform technical (evaluation of technology) and nontechnical (evaluation of people and operations) risk and vulnerability assessments of relevant technology focus areas (e.g., local computing environment, network and infrastructure, enclave boundary, supporting infrastructure, and applications).	Absent
	Make recommendations regarding the selection of cost-effective security controls to mitigate risk (e.g., protection of information, systems and processes).	Absent
Threat/Warning Analyst	Answer requests for information.	Absent
	Provide subject matter expertise to the development of a common operational picture.	Absent
	Maintain a common intelligence picture.	Absent
	Provide subject matter expertise to the development of cyber operations specific indicators.	Absent
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Absent
	Assist in the identification of intelligence collection shortfalls.	Absent
	Brief threat and/or target current situations.	Absent
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Conduct in-depth research and analysis.	Absent
	Conduct nodal analysis.	Absent
	Develop information requirements necessary for answering priority information requests.	Absent
	Evaluate threat decision-making processes.	Absent
	Identify threats to Blue Force vulnerabilities.	Absent
	Generate requests for information.	Absent
	Identify threat tactics, and methodologies.	Absent
	Identify intelligence gaps and shortfalls.	Absent
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Absent
	Monitor and report on validated threat activities.	Absent
	Monitor open source websites for hostile content directed towards organizational or partner interests.	Absent
	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Absent

	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Absent
	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Absent
	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Absent
	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Absent
	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	Absent
	Report intelligence-derived significant network events and intrusions.	Absent
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Absent
Exploitation Analyst	Conduct and/or support authorized penetration testing on enterprise network assets.	Absent
	Perform penetration testing as required for new or updated applications.	Absent
	Apply and utilize authorized cyber capabilities to enable access to targeted networks.	Absent
	Apply cyber collection, environment preparation and engagement expertise to enable new exploitation and/or continued collection operations, or in support of customer requirements.	Absent
	Apply and obey applicable statutes, laws, regulations and policies.	Absent
	Perform analysis for target infrastructure exploitation activities.	Absent
	Collaborate with other internal and external partner organizations on target access and operational issues.	Absent
	Communicate new developments, breakthroughs, challenges and lessons learned to leadership, and internal and external customers.	Absent
	Conduct analysis of physical and logical digital technologies (e.g., wireless, SCADA, telecom) to identify potential avenues of access.	Absent
	Conduct independent in-depth target and technical analysis including target-specific information (e.g., cultural, organizational, political) that results in access.	Absent
	Create comprehensive exploitation strategies that identify exploitable technical or operational vulnerabilities.	Absent
	Examine intercept-related metadata and content with an understanding of targeting significance.	Absent
	Collaborate with developers, conveying target and technical knowledge in tool requirements submissions, to enhance tool development.	Absent
	Identify gaps in our understanding of target technology and developing innovative collection approaches.	Absent

	Identify, locate, and track targets via geospatial analysis techniques.	Absent
	Lead or enable exploitation operations in support of organization objectives and target requirements.	Absent
	Maintain awareness of advancements in hardware and software technologies (e.g., attend training or conferences, reading) and their potential implications.	Absent
	Monitor target networks to provide indications and warning of target communications changes or processing failures.	Absent
	Produce network reconstructions.	Absent
	Profile network or system administrators and their activities.	Absent
All-Source Analyst	Answer requests for information.	Absent
	Provide expertise to course of action development.	Absent
	Provide subject matter expertise to the development of a common operational picture.	Absent
	Maintain a common intelligence picture.	Absent
	Provide subject matter expertise to the development of cyber operations specific indicators.	Absent
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Absent
	Assist in the identification of intelligence collection shortfalls.	Absent
	Brief threat and/or target current situations.	Absent
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Conduct in-depth research and analysis.	Absent
	Conduct nodal analysis.	Absent
	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	Absent
	Develop information requirements necessary for answering priority information requests.	Absent
	Engage customers to understand customers' intelligence needs and wants.	Absent
	Evaluate threat decision-making processes.	Absent
	Identify threat vulnerabilities.	Absent
	Identify threats to Blue Force vulnerabilities.	Absent
	Generate requests for information.	Absent
	Identify threat tactics, and methodologies.	Absent
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Absent
	Identify and submit intelligence requirements for the purposes of designating priority information requirements.	Absent
	Identify intelligence gaps and shortfalls.	Absent
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Absent
	Monitor and report on validated threat activities.	Absent
	Monitor open source websites for hostile content directed towards organizational or partner interests.	Absent

	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Absent
	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Provide subject matter expertise to website characterizations.	Absent
	Provide analyses and support for effectiveness assessment.	Absent
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Absent
	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Absent
	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Absent
	Provide input and assist in post-action effectiveness assessments.	Absent
	Provide input and assist in the development of plans and guidance.	Absent
	Provide intelligence analysis and support to designated exercises, planning activities, and time sensitive operations.	Absent
	Provide target recommendations which meet leadership objectives.	Absent
	Provide timely notice of imminent or hostile intentions or activities which may impact organization objectives, resources, or capabilities.	Absent
	Report intelligence-derived significant network events and intrusions.	Absent
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Absent
Mission Assessment Specialist	Provide expertise to course of action development.	Absent
	Provide subject matter expertise to the development of a common operational picture.	Absent
	Provide subject matter expertise to the development of cyber operations specific indicators.	Absent
	Assist in the coordination, validation, and management of all-source collection requirements, plans, and/or activities.	Absent
	Provide expertise to the development of measures of effectiveness and measures of performance.	Absent
	Assist in the identification of intelligence collection shortfalls.	Absent
	Brief threat and/or target current situations.	Absent
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Conduct end-of-operations assessments.	Absent
	Conduct in-depth research and analysis.	Absent
	Conduct nodal analysis.	Absent
	Conduct target research and analysis.	Absent
	Develop information requirements necessary for answering priority information requests.	Absent

	Develop measures of effectiveness and measures of performance.	Absent
	Develop munitions effectiveness assessment or operational assessment materials.	Absent
	Engage customers to understand customers' intelligence needs and wants.	Absent
	Estimate operational effects generated through cyber activities.	Absent
	Evaluate threat decision-making processes.	Absent
	Identify threat vulnerabilities.	Absent
	Generate requests for information.	Absent
	Identify intelligence gaps and shortfalls.	Absent
	Monitor and report changes in threat dispositions, activities, tactics, capabilities, objectives, etc. as related to designated cyber operations warning problem sets.	Absent
	Monitor and report on validated threat activities.	Absent
	Monitor operational environment and report on adversarial activities which fulfill leadership's priority information requirements.	Absent
	Produce timely, fused, all-source cyber operations intelligence and/or indications and warnings intelligence products (e.g., threat assessments, briefings, intelligence studies, country studies).	Absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Provide analyses and support for effectiveness assessment.	Absent
	Provide current intelligence support to critical internal/external stakeholders as appropriate.	Absent
	Provide evaluation and feedback necessary for improving intelligence production, intelligence reporting, collection requirements, and operations.	Absent
	Provide information and assessments for the purposes of informing leadership and customers; developing and refining objectives; supporting operation planning and execution; and assessing the effects of operations.	Absent
	Provide input and assist in post-action effectiveness assessments.	Absent
	Provide input and assist in the development of plans and guidance.	Absent
	Provide effectiveness support to designated exercises, and/or time sensitive operations.	Absent
	Provide target recommendations which meet leadership objectives.	Absent
	Work closely with planners, intelligence analysts, and collection managers to ensure intelligence requirements and collection plans are accurate and up-to-date.	Absent
Target Developer	Accurately characterize targets.	Absent
	Provide expertise to course of action development.	Absent
	Provide expertise to the development of measures of effectiveness and measures of performance.	Absent
	Build and maintain electronic target folders.	Absent
	Collaborate with intelligence analysts/targeting organizations involved in related areas.	Absent
	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Absent
	Conduct nodal analysis.	Absent

	Conduct target research and analysis.	Absent
	Coordinate target vetting with appropriate partners.	Absent
	Maintain awareness of internal and external cyber organization structures, strengths, and employments of staffing and technology.	Absent
	Determine what technologies are used by a given target.	Absent
	Develop all-source intelligence targeting materials.	Absent
	Develop measures of effectiveness and measures of performance.	Absent
	Develop munitions effectiveness assessment or operational assessment materials.	Absent
	Estimate operational effects generated through cyber activities.	Absent
	Evaluate available capabilities against desired effects to recommend efficient solutions.	Absent
	Generate requests for information.	Absent
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Absent
	Identify critical target elements.	Absent
	Initiate requests to guide tasking and assist with collection management.	Absent
	Maintain target lists (i.e., RTL, JTL, CTL, etc.).	Absent
	Perform targeting automation activities.	Absent
	Characterize websites.	Absent
	Produce target system analysis products.	Absent
	Provide aim point and reengagement recommendations.	Absent
	Provide analyses and support for effectiveness assessment.	Absent
	Provide input for targeting effectiveness assessments for leadership acceptance.	Absent
	Provide operations and reengagement recommendations.	Absent
	Provide target recommendations which meet leadership objectives.	Absent
	Provide targeting products and targeting support as designated.	Absent
	Provide time sensitive targeting support.	Absent
	Review appropriate information sources to determine validity and relevance of information gathered.	Absent
	Sanitize and minimize information to protect sources and methods.	Absent
	Support identification and documentation of collateral effects.	Absent
	Work closely with planners, analysts, and collection managers to identify intelligence gaps and ensure intelligence requirements are accurate and up-to-date.	Absent
Target Network Analyst	Provide expertise to course of action development.	Absent
	Classify documents in accordance with classification guidelines.	Absent
	Collaborate with other customer, Intelligence and targeting organizations involved in related cyber areas.	Absent
	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	Absent
	Identify and conduct analysis of target communications to identify information essential to support operations.	Absent
	Conduct nodal analysis.	Absent

	Conduct quality control to determine validity and relevance of information gathered about networks.	Absent
	Conduct target research and analysis.	Absent
	Determine what technologies are used by a given target.	Absent
	Apply analytic techniques to gain more target information.	Absent
	Generate and evaluate the effectiveness of network analysis strategies.	Absent
	Gather information about networks through traditional and alternative techniques, (e.g., social network analysis, call-chaining, traffic analysis.)	Absent
	Generate requests for information.	Absent
	Identify and evaluate threat critical capabilities, requirements, and vulnerabilities.	Absent
	Identify collection gaps and potential collection strategies against targets.	Absent
	Identify network components and their functionality to enable analysis and target development.	Absent
	Make recommendations to guide collection in support of customer requirements.	Absent
	Provide subject matter expertise to development of exercises.	Absent
	Perform content and/or metadata analysis to meet organization objectives.	Absent
	Profile targets and their activities.	Absent
	Provide target recommendations which meet leadership objectives.	Absent
	Review appropriate information sources to determine validity and relevance of information gathered.	Absent
	Reconstruct networks in diagram or report format.	Absent
	Research communications trends in emerging technologies (in computer and telephony networks, satellite, cable, and wireless) in both open and classified sources.	Absent
Multi-Disciplined Language Analyst	Compile, integrate, and/or interpret all-source data for intelligence or vulnerability value with respect to specific targets.	Absent
	Determine what technologies are used by a given target.	Absent
	Identify collection gaps and potential collection strategies against targets.	Absent
	Make recommendations to guide collection in support of customer requirements.	Absent
	Provide subject-matter expertise and support to planning/developmental forums and working groups as appropriate.	Absent
	Advise managers and operators on language and cultural issues that impact organization objectives.	Absent
	Analyze and process information using language and/or cultural expertise.	Absent
	Assess, document, and apply a target's motivation and/or frame of reference to facilitate analysis, targeting and collection opportunities.	Absent
	Collaborate across internal and/or external organizational lines to enhance collection, analysis and dissemination.	Absent
	Conduct all-source target research to include the use of open source materials in the target language.	Absent
	Conduct analysis of target communications to identify essential information in support of organization objectives.	Absent

	Perform quality review and provide feedback on transcribed or translated materials.	Absent
	Evaluate and interpret metadata to look for patterns, anomalies, or events, thereby optimizing targeting, analysis and processing.	Absent
	Identify cyber threat tactics and methodologies.	Absent
	Identify target communications within the global network.	Absent
	Maintain awareness of target communication tools, techniques, and the characteristics of target communication networks (e.g., capacity, functionality, paths, critical nodes) and their potential implications for targeting, collection, and analysis.	Absent
	Provide feedback to collection managers to enhance future collection and analysis.	Absent
	Perform foreign language and dialect identification in initial source data.	Absent
	Perform or support technical network analysis and mapping.	Absent
	Provide requirements and feedback to optimize the development of language processing tools.	Absent
	Perform social network analysis and document as appropriate.	Absent
	Scan, identify and prioritize target graphic (including machine-to-machine communications) and/or voice language material.	Absent
	Tip critical or time-sensitive information to appropriate customers.	Absent
	Transcribe target voice materials in the target language.	Absent
	Translate (e.g., verbatim, gist, and/or summaries) target graphic material.	Absent
	Translate (e.g., verbatim, gist, and/or summaries) target voice material.	Absent
	Identify foreign language terminology within computer programs (e.g., comments, variable names).	Absent
	Provide near-real time language analysis support (e.g., live operations).	Absent
	Identify cyber/technology-related terminology in the target language.	Absent
All Source-Collection Manager	Adjust collection operations or collection plan to address identified issues/challenges and to synchronize collections with overall operational requirements.	Absent
	Analyze feedback to determine extent to which collection products and services are meeting requirements.	Absent
	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements).	Absent
	Assess and apply operational environment factors and risks to collection management process.	Absent
	Assess performance of collection assets against prescribed specifications.	Absent
	Compare allocated and available assets to collection demand as expressed through requirements.	Absent
	Compile lessons learned from collection management activity's execution of organization collection objectives.	Absent
	Consider efficiency and effectiveness of collection assets and resources if/when applied against priority information requirements.	Absent

	Construct collection plans and matrixes using established guidance and procedures.	Absent
	Coordinate resource allocation of collection assets against prioritized collection requirements with collection discipline leads.	Absent
	Coordinate inclusion of collection plan in appropriate documentation.	Absent
	Re-task or re-direct collection assets and resources.	Absent
	Determine course of action for addressing changes to objectives, guidance, and operational environment.	Absent
	Determine existing collection management webpage databases, libraries and storehouses.	Absent
	Determine how identified factors affect the tasking, collection, processing, exploitation and dissemination architecture's form and function.	Absent
	Determine organizations and/or echelons with collection authority over all accessible collection assets.	Absent
	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	Absent
	Develop coordinating instructions by collection discipline for each phase of an operation.	Absent
	Allocate collection assets based on leadership's guidance, priorities, and/or operational emphasis.	Absent
	Disseminate tasking messages and collection plans.	Absent
	Establish alternative processing, exploitation and dissemination pathways to address identified issues or problems.	Absent
	Establish processing, exploitation and dissemination management activity using approved guidance and/or procedures.	Absent
	Facilitate continuously updated intelligence, surveillance, and visualization input to common operational picture managers.	Absent
	Formulate collection strategies based on knowledge of available intelligence discipline capabilities and gathering methods that align multi-discipline collection capabilities and accesses with targets and their observables.	Absent
	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	Absent
	Identify coordination requirements and procedures with designated collection authorities.	Absent
	Identify issues or problems that can disrupt and/or degrade processing, exploitation and dissemination architecture effectiveness.	Absent
	Identify potential collection disciplines for application against priority information requirements.	Absent
	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	Absent
	Issue requests for information.	Absent
	Link priority collection requirements to optimal assets and resources.	Absent
	Monitor completion of reallocated collection efforts.	Absent
	Monitor operational status and effectiveness of the processing, exploitation and dissemination architecture.	Absent

	Monitor the operational environment for potential factors and risks to the collection operation management process.	Absent
	Optimize mix of collection assets and resources to increase effectiveness and efficiency against essential information associated with priority intelligence requirements.	Absent
	Prioritize collection requirements for collection platforms based on platform capabilities.	Absent
	Provide advice/assistance to operations and intelligence decision makers with reassignment of collection assets and resources in response to dynamic operational situations.	Absent
	Request discipline-specific processing, exploitation, and disseminate information collected using discipline's collection assets and resources in accordance with approved guidance and/or procedures.	Absent
	Review capabilities of allocated collection assets.	Absent
	Review intelligence collection guidance for accuracy/applicability.	Absent
	Review list of prioritized collection requirements and essential information.	Absent
	Review and update overarching collection plan, as required.	Absent
	Revise collection matrix based on availability of optimal assets and resources.	Absent
	Specify changes to collection plan and/or operational environment that necessitate re-tasking or re-directing of collection assets and resources.	Absent
	Specify discipline-specific collections and/or taskings that must be executed in the near term.	Absent
	Synchronize the integrated employment of all available organic and partner intelligence collection assets using available collaboration capabilities and techniques.	Absent
All Source-Collection Requirements Manager	Analyze feedback to determine extent to which collection products and services are meeting requirements.	Absent
	Analyze incoming collection requests.	Absent
	Analyze plans, directives, guidance and policy for factors that would influence collection management's operational structure and requirement s (e.g., duration, scope, communication requirements, interagency/international agreements).	Absent
	Assess efficiency of existing information exchange and management systems.	Absent
	Assess performance of collection assets against prescribed specifications.	Absent
	Assess the effectiveness of collections in satisfying priority information gaps, using available capabilities and methods, and adjust collection strategies and collection requirements accordingly.	Absent
	Close requests for information once satisfied.	Absent
	Collaborate with customer to define information requirements.	Absent
	Compile lessons learned from collection management activity's execution of organization collection objectives.	Absent
	Conduct formal and informal coordination of collection requirements in accordance with established guidelines and procedures.	Absent
	Develop a method for comparing collection reports to outstanding requirements to identify information gaps.	Absent
	Develop procedures for providing feedback to collection managers, asset managers, and processing, exploitation and dissemination centers.	Absent

	Disseminate reports to inform decision makers on collection issues.	Absent
	Conduct and document an assessment of the collection results using established procedures.	Absent
	Validate the link between collection requests and critical information requirements and priority intelligence requirements of leadership.	Absent
	Evaluate extent to which collected information and/or produced intelligence satisfy information requests.	Absent
	Evaluate extent to which collection operations are synchronized with operational requirements.	Absent
	Evaluate the effectiveness of collection operations against the collection plan.	Absent
	Identify collaboration forums that can serve as mechanisms for coordinating processes, functions, and outputs with specified organizations and functional groups.	Absent
	Identify and mitigate risks to collection management ability to support the plan, operations and target cycle.	Absent
	Inform stakeholders (e.g., collection managers, asset managers, processing, exploitation and dissemination centers) of evaluation results using established procedures.	Absent
	Issue requests for information.	Absent
	Modify collection requirements as necessary.	Absent
	Provide advisory and advocacy support to promote collection planning as an integrated component of the strategic campaign plans and other adaptive plans.	Absent
	Review capabilities of allocated collection assets.	Absent
	Review intelligence collection guidance for accuracy/applicability.	Absent
	Review list of prioritized collection requirements and essential information.	Absent
	Solicit and manage to completion feedback from requestors on quality, timeliness, and effectiveness of collection against collection requirements.	Absent
	Submit information requests to collection requirement management section for processing as collection requests.	Absent
	Track status of information requests, including those processed as collection requests and production requirements, using established procedures.	Absent
	Translate collection requests into applicable discipline-specific collection requirements.	Absent
	Use feedback results (e.g., lesson learned) to identify opportunities to improve collection management efficiency and effectiveness.	Absent
	Validate requests for information according to established criteria.	Absent
Cyber Intel Planner	Provide input to the analysis, design, development or acquisition of capabilities used for meeting objectives.	Absent
	Coordinate for intelligence support to operational planning activities.	Absent
	Assess all-source intelligence and recommend targets to support cyber operation objectives.	Absent
	Assess target vulnerabilities and/or operational capabilities to determine course of action.	Absent
	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Absent

	Assist in the development and refinement of priority information requirements.	Absent
	Enable synchronization of intelligence support plans across partner organizations as required.	Absent
	Provide input to the identification of cyber-related success criteria.	Absent
	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).	Absent
	Contribute to crisis action planning for cyber operations.	Absent
	Contribute to the development of the organization's decision support tools if necessary.	Absent
	Incorporate intelligence equities into the overall design of cyber operations plans.	Absent
	Coordinate with intelligence planners to ensure that collection managers receive information requirements.	Absent
	Coordinate with the intelligence planning team to assess capability to satisfy assigned intelligence tasks.	Absent
	Coordinate, produce, and track intelligence requirements.	Absent
	Coordinate, synchronize and draft applicable intelligence sections of cyber operations plans.	Absent
	Use intelligence estimates to counter potential target actions.	Absent
	Determine indicators (e.g., measures of effectiveness) that are best suited to specific cyber operation objectives.	Absent
	Develop and review intelligence guidance for integration into supporting cyber operations planning and execution.	Absent
	Develop detailed intelligence support to cyber operations requirements.	Absent
	Develop potential courses of action.	Absent
	Develop, implement, and recommend changes to appropriate planning procedures and policies.	Absent
	Draft cyber intelligence collection and production requirements.	Absent
	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	Absent
	Evaluate intelligence estimates to support the planning cycle.	Absent
	Evaluate the conditions that affect employment of available cyber intelligence capabilities.	Absent
	Incorporate intelligence and counterintelligence to support plan development.	Absent
	Identify all available partner intelligence capabilities and limitations supporting cyber operations.	Absent
	Identify, draft, evaluate, and prioritize relevant intelligence or information requirements.	Absent
	Identify cyber intelligence gaps and shortfalls for cyber operational planning.	Absent
	Identify the need, scope, and timeframe for applicable intelligence environment preparation derived production.	Absent
	Provide input to or develop courses of action based on threat factors.	Absent

	Interpret environment preparations assessments to determine a course of action.	Absent
	Issue requests for information.	Absent
	Lead and coordinate intelligence support to operational planning.	Absent
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Absent
	Maintain situational awareness to determine if changes to the operating environment require review of the plan.	Absent
	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
	Prepare for and provide subject matter expertise to exercises.	Absent
	Provide cyber focused guidance and advice on intelligence support plan inputs.	Absent
	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	Absent
	Review and comprehend organizational leadership objectives and guidance for planning.	Absent
	Scope the cyber intelligence planning effort.	Absent
	Document lessons learned that convey the results of events and/or exercises.	Absent
Cyber Ops Planner	Ensure that intelligence planning activities are integrated and synchronized with operational planning timelines.	Absent
	Evaluate intelligence estimates to support the planning cycle.	Absent
	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Absent
	Gather and analyze data (e.g., measures of effectiveness) to determine effectiveness, and provide reporting for follow-on activities.	Absent
	Incorporate cyber operations and communications security support plans into organization objectives.	Absent
	Identify cyber intelligence gaps and shortfalls for cyber operational planning.	Absent
	Integrate cyber planning/targeting efforts with other organizations.	Absent
	Interpret environment preparations assessments to determine a course of action.	Absent
	Issue requests for information.	Absent
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Absent
	Maintain situational awareness of cyber-related intelligence requirements and associated tasking.	Absent
	Maintain situational awareness of partner capabilities and activities.	Absent
	Maintain situational awareness to determine if changes to the operating environment require review of the plan.	Absent
	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent

	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	Absent
	Prepare for and provide subject matter expertise to exercises.	Absent
	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	Absent
	Provide input to the administrative and logistical elements of an operational support plan.	Absent
	Provide planning support between internal and external partners.	Absent
	Recommend refinement, adaption, termination, and execution of operational plans as appropriate.	Absent
	Review, approve, prioritize, and submit operational requirements for research, development, and/or acquisition of cyber capabilities.	Absent
	Submit or respond to requests for deconfliction of cyber operations.	Absent
	Document lessons learned that convey the results of events and/or exercises.	Absent
Partner Integration Planner	Apply expertise in policy and processes to facilitate the development, negotiation, and internal staffing of plans and/or memorandums of agreement.	Absent
	Assist and advise interagency partners in identifying and developing best practices for facilitating operational support to achievement of organization objectives.	Absent
	Provide expertise to course of action development.	Absent
	Collaborate with other team members or partner organizations to develop a diverse program of information materials (e.g., web pages, briefings, print materials).	Absent
	Contribute to crisis action planning for cyber operations.	Absent
	Contribute to the development, staffing, and coordination of cyber operations policies, performance standards, plans and approval packages with appropriate internal and/or external decision makers.	Absent
	Coordinate with intelligence and cyber defense partners to obtain relevant essential information.	Absent
	Develop or participate in the development of standards for providing, requesting, and/or obtaining support from external partners to synchronize cyber operations.	Absent
	Develop or shape international cyber engagement strategies, policies, and activities to meet organization objectives.	Absent
	Develop strategy and processes for partner planning, operations, and capability development.	Absent
	Develop, implement, and recommend changes to appropriate planning procedures and policies.	Absent
	Develop, maintain, and assess cyber cooperation security agreements with external partners.	Absent
	Facilitate interactions between internal and external partner decision makers to synchronize and integrate courses of action in support of objectives.	Absent
	Facilitate the sharing of “best practices” and “lessons learned” throughout the cyber operations community.	Absent
	Identify and manage security cooperation priorities with external partners.	Absent

	Inform external partners of the potential effects of new or revised policy and guidance on cyber operations partnering activities.	Absent
	Integrate cyber planning/targeting efforts with other organizations.	Absent
	Maintain relationships with internal and external partners involved in cyber planning or related areas.	Absent
	Monitor and evaluate integrated cyber operations to identify opportunities to meet organization objectives.	Absent
	Contribute to the review and refinement of policy, to include assessments of the consequences of endorsing or not endorsing such policy.	Absent
	Provide subject matter expertise to planning teams, coordination groups, and task forces as necessary.	Absent
	Conduct long-range, strategic planning efforts with internal and external partners in cyber activities.	Absent
	Provide subject matter expertise to planning efforts with internal and external cyber operations partners.	Absent
	Propose policy which governs interactions with external coordination groups.	Absent
	Prepare for and provide subject matter expertise to exercises.	Absent
	Provide cyber focused guidance and advice on intelligence support plan inputs.	Absent
	Provide input for the development and refinement of the cyber operations objectives, priorities, strategies, plans, and programs.	Absent
	Provide planning support between internal and external partners.	Absent
	Serve as a conduit of information from partner teams by identifying subject matter experts who can assist in the investigation of complex or unusual situations.	Absent
	Serve as a liaison with external partners.	Absent
	Submit or respond to requests for deconfliction of cyber operations.	Absent
	Synchronize cyber international engagement activities and associated resource requirements as appropriate.	Absent
	Synchronize cyber portions of security cooperation plans.	Absent
	Document lessons learned that convey the results of events and/or exercises.	Absent
Cyber Operator	Analyze internal operational architecture, tools, and procedures for ways to improve performance.	Absent
	Analyze target operational architecture for ways to gain access.	Absent
	Collaborate with development organizations to create and deploy the tools needed to achieve objectives.	Absent
	Conduct access enabling of wireless computer and digital networks.	Absent
	Conduct collection and processing of wireless computer and digital networks.	Absent
	Conduct exploitation of wireless computer and digital networks.	Absent
	Conduct network scouting and vulnerability analyses of systems within a network.	Absent
	Conduct on-net activities to control and exfiltrate data from deployed technologies.	Absent
	Conduct on-net and off-net activities to control, and exfiltrate data from deployed, automated technologies.	Absent
	Conduct open source data collection via various online tools.	Absent

	Conduct survey of computer and digital networks.	Absent
	Deploy tools to a target and utilize them once deployed (e.g., backdoors, sniffers).	Absent
	Detect exploits against targeted networks and hosts and react accordingly.	Absent
	Develop new techniques for gaining and keeping access to target systems.	Absent
	Edit or execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems.	Absent
	Exploit network devices, security devices, and/or terminals or environments using various methods or tools.	Absent
	Facilitate access enabling by physical and/or wireless means.	Absent
	Identify potential points of strength and vulnerability within a network.	Absent
	Maintain situational awareness and functionality of organic operational infrastructure.	Absent
	Operate and maintain automated systems for gaining and maintaining access to target systems.	Absent
	Conduct cyber activities to degrade/remove information resident in computers and computer networks.	Absent
	Process exfiltrated data for analysis and/or dissemination to customers.	Absent
	Provide real-time actionable geolocation information.	Absent
	Record information collection and/or environment preparation activities against targets during operations designed to achieve cyber effects.	Absent
	Test and evaluate locally developed tools for operational use.	Absent
	Test internal developed tools and techniques against target tools.	Absent
Cyber Crime Investigator	Conduct interviews of victims and witnesses and conduct interviews or interrogations of suspects.	Absent
	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.	Absent
	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).	Absent
	Examine recovered data for information of relevance to the issue at hand.	Absent
	Fuse computer network attack analyses with criminal and counterintelligence investigations and operations.	Absent
	Identify and/or determine whether a security incident is indicative of a violation of law that requires specific legal action.	Absent
	Identify data or intelligence of evidentiary value to support counterintelligence and criminal investigations.	Absent
	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Absent
	Identify elements of proof of the crime.	Absent
	Identify, collect, and seize documentary or physical evidence, to include digital media and logs associated with cyber intrusion incidents, investigations, and operations.	Absent
	Process crime scenes.	Absent
	Secure the electronic device or information source.	Absent

	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Absent
	Analyze the crisis to ensure public, personal, and resource protection.	Absent
	Assess the behavior of the individual victim, witness, or suspect as it relates to the investigation.	Absent
	Determine the extent of threats and recommend courses of action or countermeasures to mitigate risks.	Absent
	Provide criminal investigative support to trial counsel during the judicial process.	Absent
	Analyze computer-generated threats for counter intelligence or criminal activity.	Absent
	Gather and preserve evidence used on the prosecution of computer crimes.	Absent
	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion or other crimes.	Absent
	Determine and develop leads and identify sources of information to identify and/or prosecute the responsible parties to an intrusion or other crimes.	Absent
	Document original condition of digital and/or associated evidence (e.g., via digital photographs, written reports, hash function checking).	Absent
	Employ information technology (IT) systems and digital storage media to solve, investigate, and/or prosecute cybercrimes and fraud committed against people and property.	Absent
	Prepare reports to document the investigation following legal standards and requirements.	Absent
Law Enforcement /CounterIntelligence Forensics Analyst	Develop a plan to investigate alleged crime, violation, or suspicious activity utilizing computers and the Internet.	Absent
	Establish relationships, if applicable, between the incident response team and other groups, both internal (e.g., legal department) and external (e.g., law enforcement agencies, vendors, public relations professionals).	Absent
	Resolve conflicts in laws, regulations, policies, standards, or procedures.	Absent
	Analyze incident data for emerging trends.	Absent
	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Absent
	Acquire and maintain a working knowledge of constitutional issues which arise in relevant laws, regulations, policies, agreements, standards, procedures, or other issuances.	Absent
	Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.	Absent
	Read, interpret, write, modify, and execute simple scripts (e.g., Perl, VBScript) on Windows and UNIX systems (e.g., those that perform tasks such as: parsing large data files, automating manual tasks, and fetching/processing remote data).	Absent
	Identify and/or develop reverse engineering tools to enhance capabilities and detect vulnerabilities.	Absent
	Analyze organizational cyber policy.	Absent
	Conduct analysis of log files, evidence, and other information to determine best methods for identifying the perpetrator(s) of a network intrusion.	Absent

Cyber Defense Forensics Analyst	Confirm what is known about an intrusion and discover new information, if possible, after identifying intrusion via dynamic analysis.	Absent
	Create a forensically sound duplicate of the evidence (i.e., forensic image) that ensures the original evidence is not unintentionally modified, to use for data recovery and analysis processes. This includes, but is not limited to, hard drives, floppy diskettes, CDs, PDAs, mobile phones, GPS, and all tape formats.	Absent
	Decrypt seized data using technical means.	Absent
	Provide technical summary of findings in accordance with established reporting procedures.	Absent
	Ensure that chain of custody is followed for all digital media acquired in accordance with the Federal Rules of Evidence.	Absent
	Examine recovered data for information of relevance to the issue at hand.	Absent
	Identify digital evidence for examination and analysis in such a way as to avoid unintentional alteration.	Absent
	Perform dynamic analysis to boot an “image” of a drive (without necessarily having the original drive) to see the intrusion as the user may have seen it, in a native environment.	Absent
	Perform file signature analysis.	Absent
	Perform hash comparison against established database.	Absent
	Perform real-time forensic analysis (e.g., using Helix in conjunction with LiveView).	Absent
	Perform timeline analysis.	Absent
	Perform real-time cyber defense incident handling (e.g., forensic collections, intrusion correlation and tracking, threat analysis, and direct system remediation) tasks to support deployable Incident Response Teams (IRTs).	Absent
	Perform static media analysis.	Absent
	Perform tier 1, 2, and 3 malware analysis.	Absent
	Prepare digital media for imaging by ensuring data integrity (e.g., write blockers in accordance with standard operating procedures).	Absent
	Provide technical assistance on digital evidence matters to appropriate personnel.	Absent
	Recognize and accurately report forensic artifacts indicative of a particular operating system.	Absent
	Extract data using data carving techniques (e.g., Forensic Tool Kit [FTK], Foremost).	Absent
	Capture and analyze network traffic associated with malicious activities using network monitoring tools.	Absent
	Use specialized equipment and techniques to catalog, document, extract, collect, package, and preserve digital evidence.	Absent
	Conduct cursory binary analysis.	Absent
	Serve as technical expert and liaison to law enforcement personnel and explain incident details as required.	Absent
	Perform virus scanning on digital media.	Absent
	Perform file system forensic analysis.	Absent
	Perform static analysis to mount an "image" of a drive (without necessarily having the original drive).	Absent

	Perform static malware analysis.	Absent
	Utilize deployable forensics toolkit to support operations as necessary.	Absent
	Coordinate with intelligence analysts to correlate threat assessment data.	Absent
	Process image with appropriate tools depending on analyst's goals.	Absent
	Perform Windows registry analysis.	Absent
	Perform file and registry monitoring on the running system after identifying intrusion via dynamic analysis.	Absent
	Enter media information into tracking database (e.g., Product Tracker Tool) for digital media that has been acquired.	Absent
	Correlate incident data and perform cyber defense reporting.	Absent
	Maintain deployable cyber defense toolkit (e.g., specialized cyber defense software/hardware) to support Incident Response Team mission.	Absent
	Collect and analyze intrusion artifacts (e.g., source code, malware, and system configuration) and use discovered data to enable mitigation of potential cyber defense incidents within the enterprise.	Absent
	Review forensic images and other data sources (e.g., volatile data) for recovery of potentially relevant information.	Absent
	Write and publish cyber defense recommendations, reports, and white papers on incident findings to appropriate constituencies.	Absent

List of potential threats to GrubHub that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, cybersecurity work roles, and cybersecurity tasks.

Threats
Lack of cybersecurity policies
Threat to their critical assets
Lack of legal representatives
Lack of security preventive measures
Lack of response and mitigation policies
Lack of recovery plans
Lack of proper investigation and forensics when incidents occur

List of potential threats to GrubHub that could exploit vulnerabilities of critical assets due to missing cybersecurity specialty areas, cybersecurity work roles, and cybersecurity tasks.

Risks
Exposure of confidential information
Not discovering the root cause of attack can lead to the re-occurrence of the attack.
If attacked can lead to financial loses
Can ruin company reputation if attacked
Having no proper procedures on how to handle an attack and who should be responsible can lead to destroying the company
Availability of service. If attacked, customers won't be able to use their services.
Lack of awareness can lead to unnecessary vulnerabilities that can lead to attacks.

List of recommended policies for each recommended cybersecurity specialty areas, cybersecurity work roles, and cybersecurity tasks that should be created to mitigate the identified risks.

- The company should establish a forensics team for proper investigation when an attack occurs.
- All employees should be educated on the cybersecurity risks to avoid unnecessary vulnerabilities.
- Company should make sure that they are following the requires standard local, national, and global policies.
- Regular risk assessments should be done to ensure the company assets, threats, and vulnerabilities are fully assessed and updated to reduce risks.
- If any of the cybersecurity experts are outsourced, the company should thoroughly research their previous works to ensure they deliver the best results.

PART C: Security Risk Management Recommendations

List of recommended Prevention and Response controls, methods and policies and their implementation costs and benefits based on risk management analysis

For GrubHub:

- The use of encrypted backup incase the system gets compromised.
- Creating an incidence response plan which clearly state who is responsible for what when an incident occurs.
- Enforcing application and website to work on updated software version of user's devices to ensure transactions are done safely.
- Learning the root cause of the incident by investigation the logs.
- Secure Router Planes should be configured properly to handles more traffic and re-direct traffic when overwhelmed instead of going through a DoD.
- Application accounts should be created to ensure separation of data.
- Security structure support is already enforced but stored in the same network. It should be stored on separate networks.

Total cost and benefit in $ for the recommended controls, methods, and policies-based security risk management analysis**.**

For HGA:

Residual Risk Reduction:
= Residual Risk with current controls – Residual risk with new controls
= 845250 – 676293
=168,957
The value of residual risk reduction does not exceed the budget for the proposed controls

What is the ((proposed security risk budget cost)/ (expected security risk Benefit)) ratio for the 3 budgets from Mixed Strategy?

Cost benefit ratio analysis for risk prevention budget
=Proposed security risk budget cost/ expected security risk Benefit
=287,000/168,957
=1.70

Cost benefit ratio analysis for risk response budget
=Proposed security risk budget cost/ expected security risk Benefit
=275,000/168,957
=1.63

Cost benefit ratio analysis for Mixed budget
=Proposed security risk budget cost/ expected security risk Benefit
= 546,000/168,957
=3.23

For GrubHub:

Residual Risk Reduction:

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

= 900,000 – 300,000

=600,000

The value of residual risk reduction does not exceed the budget for the proposed controls

Cost benefit ratio analysis for Mixed budget

=Proposed security risk budget cost/ expected security risk Benefit

= 422,350/600,000

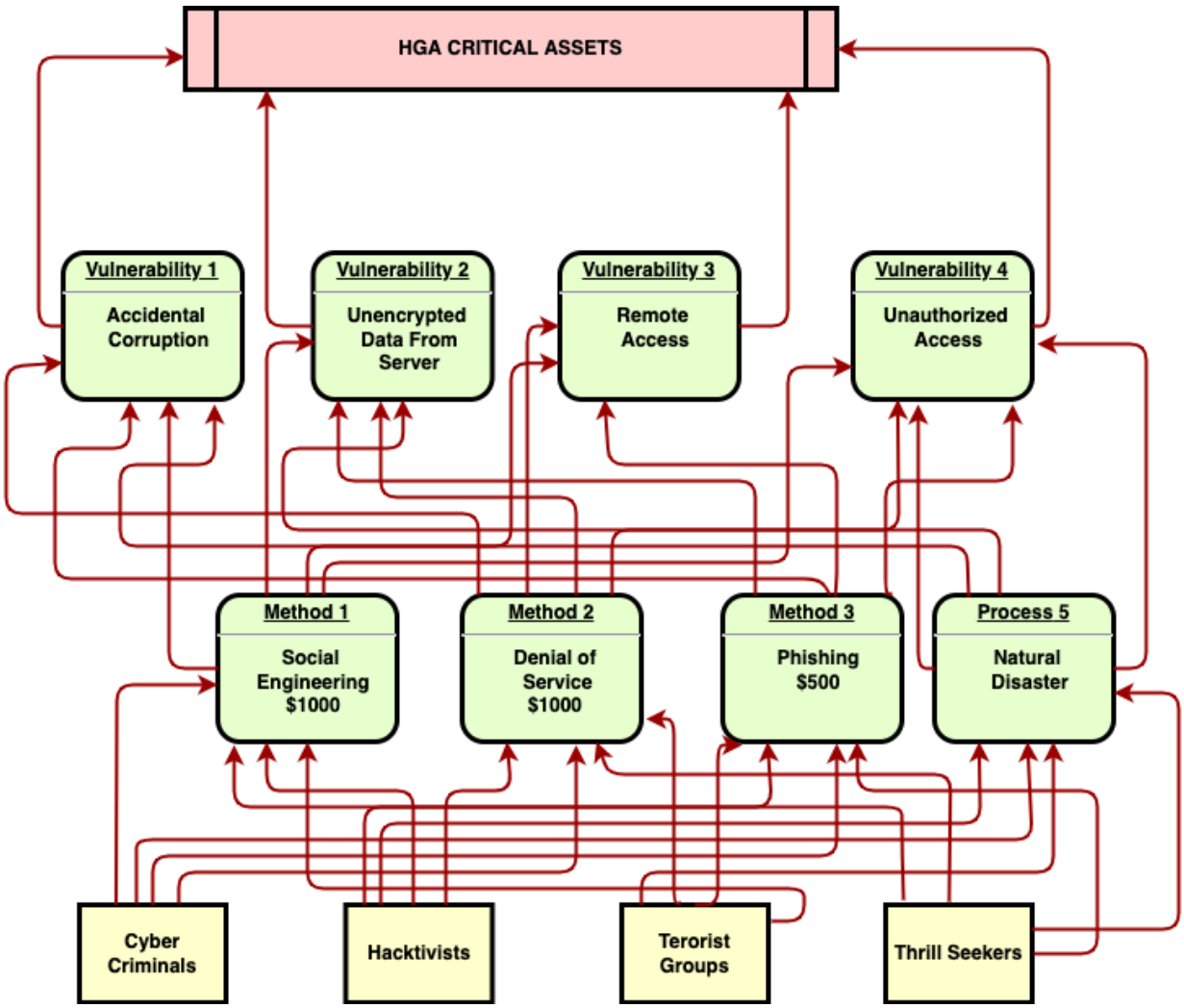
=7.04

Comparing proposed security controls, methods, and policies budget for HGA with the proposed security controls, methods, and policies budget for GrubHub.

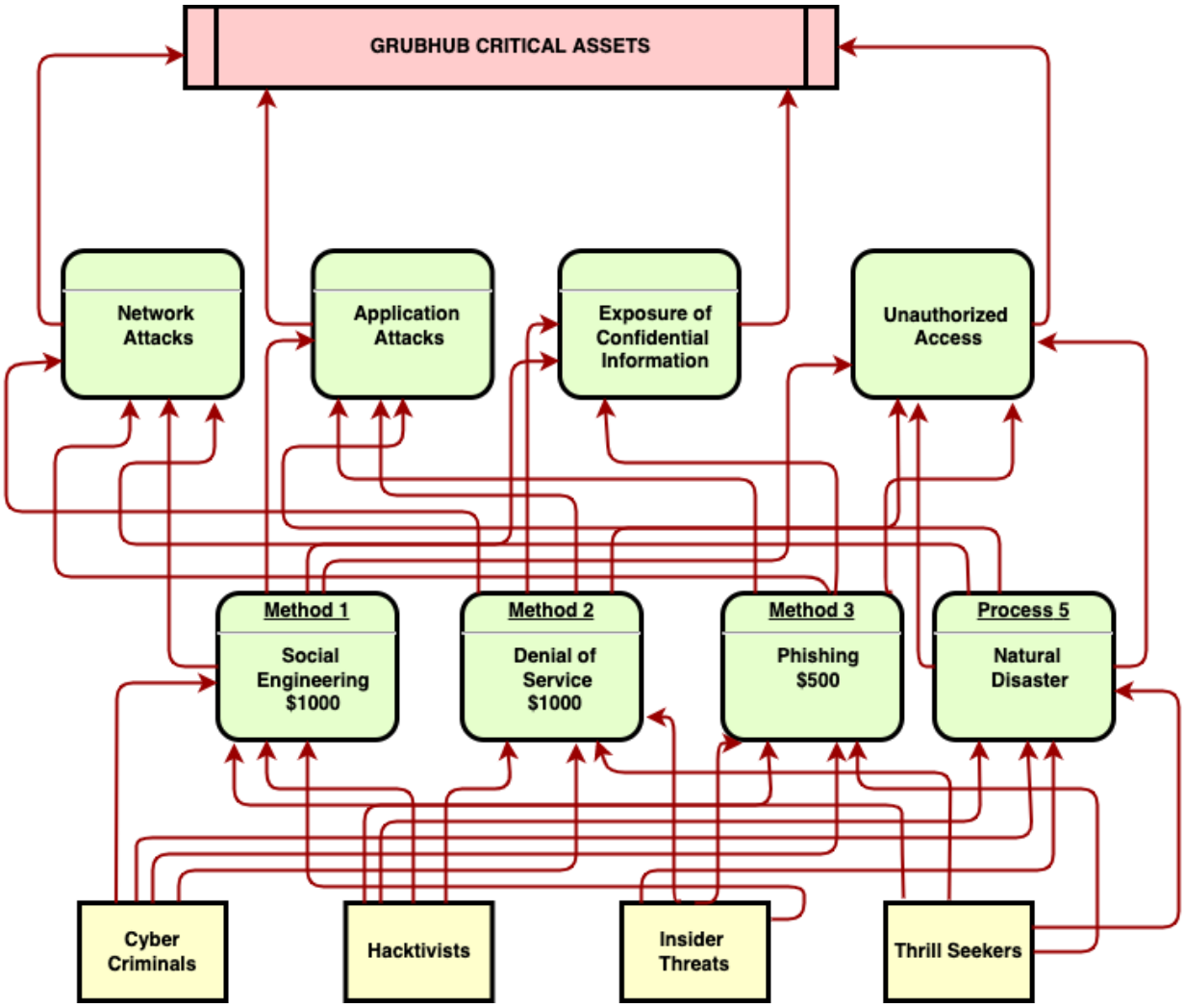
Points of Comparison	**HGA**	**GrubHub**
Industry	Government-Financial	Private – Food Delivery
Mission	Transfers paychecks based on different government sectors needs	Delivers food from various restaurants.
Geographic Presence	United States of America	USA and Canada
Number of Employees	1000	3000
Network Technology	Appendix	Appendix
Critical Assets in $	$845,250	$2,100,000
Threat Environment	Nation State, Hacker Organizations, Cyber Terrorists	Hacker Organizations, Cyber criminals, Competitors
Threat Agents	Cyber Criminals, Hacktivists, Terrorist Groups, Thrill Seekers	Cyber criminals, Insider Threats, Thrill Seekers
Residual Security Risks in $	$168,957	$85,000
Budget for risk prevention and response controls, methods, policies	$546,000	$422,350
Security Budget / Security Risk Improvement	0.89	0.63
Security Budget / Critical Assets	0.65	0.20
Security Budget / Employees	546	140.78

Attack Trees

For HGA:



For GrubHub:


GRUBHUB CRITICAL ASSETS
Network Attacks
Application Attacks
Exposure of Confidential Information
Unauthorized Access
Method 1
Social Engineering $1000
Method 2
Denial of Service $1000
Method 3
Phishing $500
Process 5
Natural Disaster
Cyber Criminals
Hacktivists
Insider Threats
Thrill Seekers

Vulnerabilities and Exploitation Probabilities:

For HGA:

Vulnerabilities	Exploitation Probability
Unauthorized Access	30
Wrong time sheets	20
Errors on time attendances or punches	35
Manager unawareness	15
Accidental corruption of data	25
Server Access Control	10
Division contingency planning	25
Eavesdropping	10
Data loss via email	20
Unencrypted data transmission from server	15
VPN vulnerability	25
Remote Access	17

For GrubHub:

Vulnerabilities	Exploitation Probability
Permanent tokens vulnerability	25
Unauthorized Access	15
Weak Authentication	10
Network based attacks	20
Impersonation – Brute force attack	15
Identity theft	25
Backdoor attack	17
Botnet attack	25
IP Spoofing	15
ARP Attack	10
DoS – Denial of Service	20
OS attacks	15

Cybersecurity workforce recommendations

For HGA:

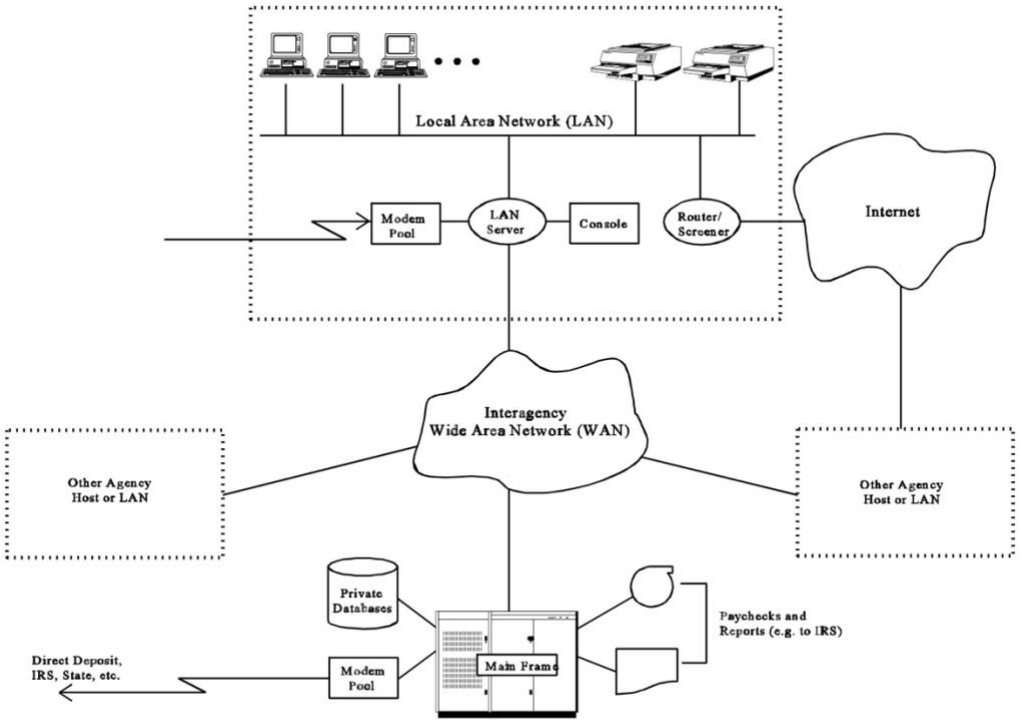
- All employees including managers should be trained regularly on safety daily security practices and how they affect their daily jobs.
- Systems should be audited regularly to ensure they are up to date with all the standard policies and that they are enforced.
- Organization should analyze any third-party systems that they plan to work with to ensure that vulnerabilities are minimized prior to the collaboration.

For GrubHub:

- Systems used should be updated regularly.
- Patches and bugs should be fixed and implemented quickly.
- A forensics team should be established to ensure attack investigations are done thoroughly.
- Risks assessments should be done regularly and if possible, should be done by a third party.

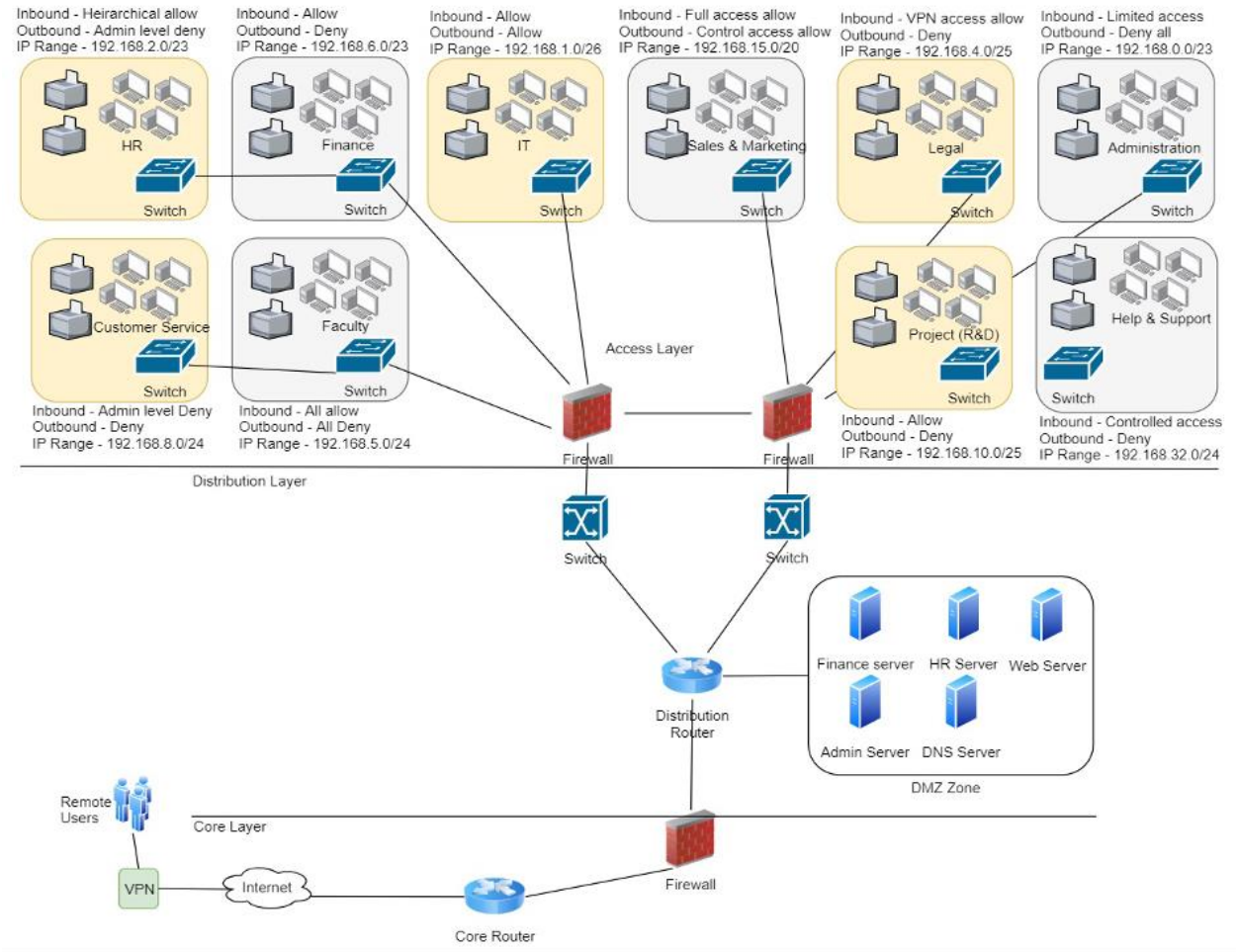
Appendix:

System Environment for HGA:



The image above represents the system architecture of HGA prior to Security Assessment. Systems are connected via LAN, with a modem pool and router for wireless connections. At HGA, we have a Main Frame that handles several tasks such as transferring payments to our customers. The Main Frame is very secured, and it connects to the private database that stores sensitive information. HGA is also connected to other organizations via WAN.

Updated Network Topology for GrubHub (defense-in-depth)



A summary explaining the network topology diagram

NB: Please note that this was designed by me in accordance with my understanding of GrubHub's network infrastructure based on the information provided by my informant. That said, it is not the actual network infrastructure used at GrubHub.

The diagram was designed with a defense in depth mindset. Thus, we have 3 designated layers (access layer, distribution layer, and core layer) with a DMZ set aside to connect the public to necessary internal information. Different departments were categorized into zones within the access layer. The diagram also illustrated different policies enforced for each department. Some have full access, some have limited access, deny all, and others have control access based on ports configurations. Additionally, the organization has a VPN that allows users to connect to internal networks from different geographical locations.

For security enforcement, firewalls have been installed between all layers of security, the company uses multiple routers and the use of DMZ to keeps confidential information away from the public.

Works Cited

(n.d.). Retrieved from beyondtrust.com: https://www.beyondtrust.com/resources/glossary/password

(2019, Sep 30). Retrieved from stigviewer.com: https://www.stigviewer.com/stig/application_security_and_development/2019-09-30/finding/V-69537

802.1X Overview and EAP Types. (2021, Oct 28). Retrieved from intel.com: https://www.intel.com/content/www/us/en/support/articles/000006999/wireless/legacy-intel-wireless-products.html

asilentkingdom. (2014, Jan 19). *BLE pairing vs. bonding.* Retrieved from piratecomm.wordpress.com: https://piratecomm.wordpress.com/2014/01/19/ble-pairing-vs-bonding/

Baseline items in Software Development. (2020, Aug 10). Retrieved from geeksforgeeks.org: https://www.geeksforgeeks.org/baseline-items-in-software-development/#:~:text=A%20baseline%20is%20milestone%20and,Baseline%20is%20shared%20project%20database.

CCMP. (n.d.). Retrieved from tech-faq: https://www.tech-faq.com/ccmp-counter-mode-with-cipher-block-chaining-message-authentication-code-protocol.html

CDPD. (2011, Aug 18). Retrieved from techopedia.com: https://www.techopedia.com/definition/5049/cellular-digital-packet-data-cdpd

Database Credentials Policy. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=2

Database Links. (n.d.). Retrieved from oracle.com: https://docs.oracle.com/cd/E18283_01/server.112/e17120/ds_concepts002.htm

Lutkevich, B. (n.d.). Retrieved from techtarget.om: https://www.techtarget.com/searchsecurity/definition/digital-signature

Network Access Control. (n.d.). Retrieved from vmware: https://www.vmware.com/topics/glossary/content/network-access-control#:~:text=Network%20access%20control%20is%20the,out%20of%20a%20private%20network.&text=Effective%20network%20access%20control%20restricts,patches%20and%20anti%2Dintrusion%20software.

Remote Access Tools Policy. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=5

Rosencrance, L. (n.d.). *Remote Access.* Retrieved from techtarget.com: https://www.techtarget.com/searchsecurity/definition/remote-access#:~:text=Remote%20access%20is%20the%20ability,they%20are%20physically%20far%20away.

Router and Switch Security Policy. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=6

RSN. (n.d.). Retrieved from tech-faq: https://www.tech-faq.com/rsn-robust-secure-network.html

Security Policy Templates. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=5

Teeling, M. (2021, May 14). *What is Data integrity.* Retrieved from veracode.com: https://www.veracode.com/blog/2012/05/what-is-data-integrity

Types of Veteran ID cards. (n.d.). Retrieved from va.gov: https://www.va.gov/records/get-veteran-id-cards/

Virtual Private Network Policy. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=6
VLAN. (n.d.). Retrieved from techtarget: https://www.techtarget.com/searchnetworking/definition/virtual-LAN#:~:text=A%20VLAN%20(virtual%20LAN)%20is,within%20the%20same%20geographical%20area.&text=A%20VLAN%20is%20associated%20with%20a%20broadcast%20domain.
VLAN Trunking Protocol. (2021, Feb 23). Retrieved from Wikipedia: https://en.wikipedia.org/wiki/VLAN_Trunking_Protocol
Web Application Security Policy. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=6
What is a Security Token. (n.d.). Retrieved from okta.com: https://www.okta.com/identity-101/security-token/#:~:text=A%20security%20token%20is%20a,the%20conduit%20for%20this%20data.
Wikipedia. (2021, Dec 1). Retrieved from wikipedia.org: https://en.wikipedia.org/wiki/Vulnerability_management
Wireless Communication Policy. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=7
Wireless Communicaton Standard. (n.d.). Retrieved from sans.org: https://www.sans.org/information-security-policy/?page=7
Yfantis, V. (2019, Jul 16). *Smart Card Authentication.* Retrieved from parallels.com: https://www.parallels.com/blogs/ras/smart-card-authentication/