



Risk Management Framework (RMF) Resource Center

www.rmfm.org

RMF DOD IT IN DEPTH PARTICIPANTS COURSE ACTIVITIES GUIDE V9.0

COURSE ACTIVITIES

Contents

THE DEPARTMENT OF ULTRA DIEHARDS (DUD) CASE STUDY	4
PREPARE	6
Activity 1: PCOMS Informal Risk Assessment Activity	6
PCOMS Program Manager Areas of Concern	7
Task 1: Areas of Concern (Vulnerabilities) Likelihood, Impact and Risk	8
Likelihood Score Table	10
Impact Score Table	10
Risk Score Key	10
Data Vulnerabilities Worksheet	11
Applications Vulnerabilities Worksheet	12
Server Vulnerabilities Worksheet	13
Infrastructure Vulnerabilities Worksheet	14
Roles and Responsibilities Vulnerabilities Worksheet	15
Task 2: Identify Medium to Extreme Risks (Areas of Concern Worksheet)	16
Task 3: Prepare a Summary Risk Score Report for Management	18
Walkthrough Analysis of PCOMS Boundary and Information Types	19
Information Types Based on the System Description	19
Information Types Based on the PCOMS Subsystem Applications	19
Information Types Based on the PCOMS Technical Overview	20
CATEGORIZE	21
Activity 2: Determine Boundary and Categorization for the LIMBO System	21
LIMBO Information System Type	21
LIMBO System Description	21
LIMBO Subsystems:	22
LIMBO Technical Overview	22
Categorize the LIMBO System	24
SELECT	25
Activity 3: Identify PCOMS Security Control Requirements	25
Activity 4: Allocate PCOMS Security Controls	29
Task 1: Allocate Security Controls - Propose Common/Inherited, Hybrid or System Specific Controls	29
Task 2: Allocate Security Controls - Assessment	35
IMPLEMENTATION/ASSESS	37
Activity 5: IMPLEMENT/ASSESS/Continuous Monitoring Activity	37

Instructions	37
AT-2 LITERACY TRAINING AND AWARENESS.....	37
CA-5 PLAN OF ACTION AND MILESTONES.....	39
IR-9 INFORMATION SPILLAGE RESPONSE.....	40
CP-7 ALTERNATE PROCESSING SITE	42
CP-9 SYSTEM BACKUP	43
PS-6 ACCESS AGREEMENTS	45
CM-3 CONFIGURATION CHANGE CONTROL	46
AT-3 ROLE-BASED TRAINING	48
RA-5 VULNERABILITY SCANNING.....	49
CP-3 CONTINGENCY TRAINING	51
PE-17 ALTERNATE WORK SITE	53
AUTHORIZE	55
Activity 6: Authorize Concepts Review Quiz	55
MONITOR	56
Activity 7: Maintaining Current Documentation during the Monitor Phase	56

THE DEPARTMENT OF ULTRA DIEHARDS (DUD) CASE STUDY

The Photography Adjustment and Management (PAM) Act of 1994 established photography collection programs and reporting mechanisms designed to enhance photographic capabilities for the US Government. The Geospatial Operations Organization (GOO) has been involved in the acquisition, use, and distribution of aerial photography for more than 35 years for DUD users.

The GOO relies on the Aerial Photography Program Management Office (AP2MO) for the acquisition, inspection, distribution and archiving of the imagery needs for GOO, DUD, and authorized federal and state agencies, and other approved DUD users and associates through the operations and management of the Photography Collection & Operations Management System (PCOMS).

GOO also has the mission of ensuring installation maintenance which includes maintaining and operating public lands, buildings, monuments, and surrounding property. This also includes activities devoted to ensuring the preservation of land, water, wildlife, and natural resources. It includes the sustainable stewardship of natural resources on federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.).

The PCOMS is hosted in the Hosting and Operations and Services Division (HOSD) mixed Linux and Microsoft Windows data center environment. As part of the hosting agreement, HOSD is responsible for providing Enterprise Active Directory (EAD), security, network, and monitoring services. AP2MO management, through AP2MO system and database administrators, is responsible for all hardware, operating systems, databases, installation, administration, authorization, purchasing and maintenance of the PCOMS application and all sub-components.

PCOMS data has been designated as highly sensitive, however, not classified. Authorized users of PCOMS will be provided access to information pertinent to their individual projects. PCOMS data will not be shared with the general public.

PCOMS end users are located nationally with secured web access to the PCOMS application.

BAI DUD Organization

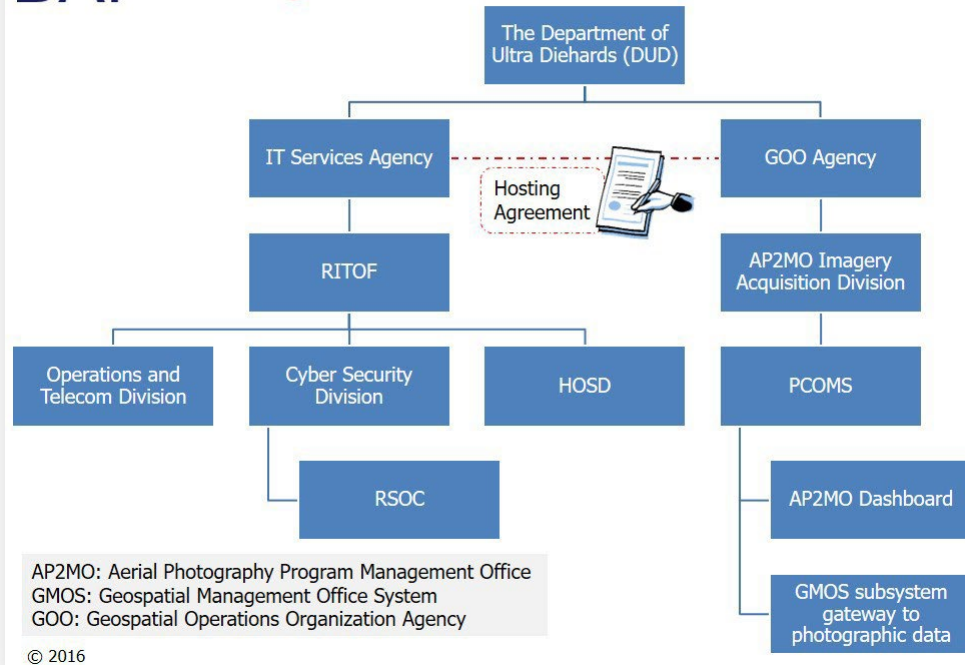


Figure 1 - Department of Ultra Diehards (DUD) Organization

BAI Overview

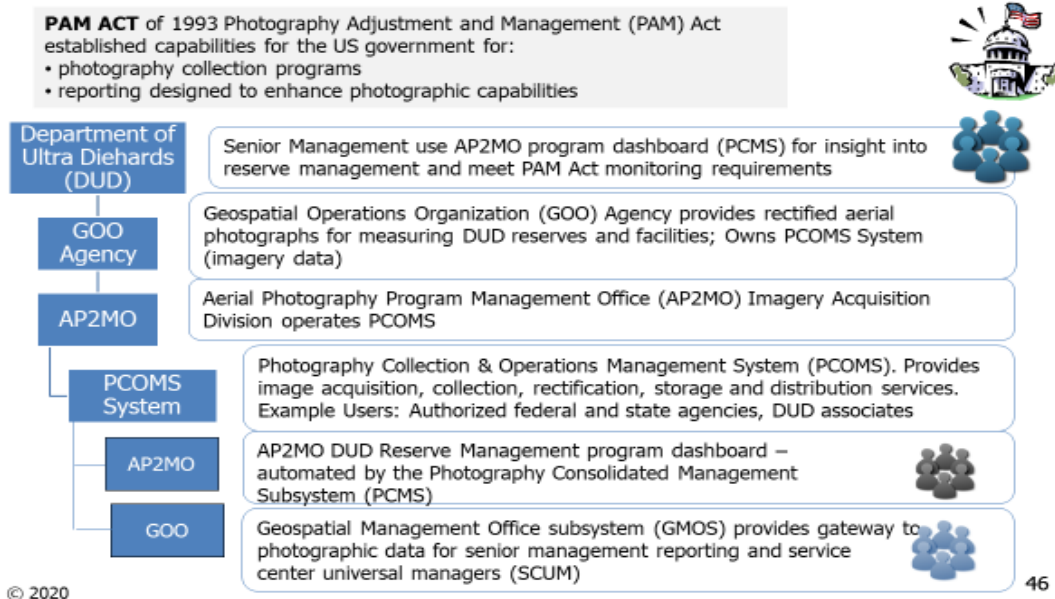


Figure 2 - Department of Ultra Diehards (DUD) Case Study

PREPARE

Activity 1: PCOMS Informal Risk Assessment Activity

The purpose of this activity is to build a basic understanding of risk assessment, risk reporting and risk management. These are essential to RMF, as understanding risk management helps in decision-making and prioritizing efforts around control implementation.

Instructions

Each team will focus on one of the five Risk areas of concern (potential vulnerabilities) identified for the PCOMS case study:

- Data
- Applications
- Servers
- Infrastructure
- Roles and Responsibilities

Resources

Your team will use the worksheet that is labeled with your team's assigned area of concern.

There are three sub-tasks in this risk assessment activity:

- Task 1: Conduct Informal Risk Analysis
- Task 2: Identify Medium to Extreme Risks
- Task 3: Produce a Summary Risk Score Report

PCOMS Program Manager Areas of Concern

The AP2MO Program Manager for PCOMS has been informed that PCOMS will have to undergo the Risk Management Framework (RMF) process to receive authorization to continue processing data for the GOO. The Program Manager has asked that you, the primary System POC, work with your team of functional, technical and security POCs associated with the application. He has asked that the team conduct an informal risk assessment on PCOMS to understand the basic threats, vulnerabilities, and possible risks.

He went on to explain his areas of concern as they relate to the PCOMS application and obtaining an authorization for RMF.

1. PCOMS is housed in the HOSD Data Center. HOSD resides on a military base secured with guards and visitor procedures. The brick building is strong however the datacenter resides in the basement. The area has a high frequency of summer storms and potential of tornadoes. Also, the base sits on a 100-yr flood plain which means a major flood only occurs approximately every 100 years. But there are no flood walls.
2. Although he pays for the use of the HOSD data center, he has concerns regarding fire as there are several different organizations in the building, and it was noticed (by the PCOMS Systems Admin) that the fire inspection report is over a year old. In addition, there was a power outage recently and not all machines were able to be restored at the same time. Due to these lapses in protection, should he be worried about other physical vulnerabilities in the HOSD?
3. The AP2MO Information Systems Security Manager has noticed some expirations in certifications for the PCOMS IT support staff (i.e. System Admins, etc.). Could this be an indicator of a larger problem with certain IT staff members? Lack of responsibility or capability in the System Admin staff could lead to Insider Threats.
4. The loss of personnel through multiple retirements over the last year has created a gap in unfilled positions involved with the configuration management process. This also includes some personnel in the HOSD. The Program Manager is concerned that the CM process may be broken.
5. The PCOMS data is highly sensitive. Although he feels the servers are well protected, he is concerned that the users (not located with PCOMS) could be a risk. He questions their basic training requirements.
6. Also, because of data sensitivity, there is always the concern of the Advanced Persistent Threat (APT) from our adversaries. The PM wants to make sure all vulnerable areas are reviewed and secured.

7. Application development is outsourced to outside contractors. The PM wants to make sure that proper application design guidelines are being followed regarding design review, revision control, and use of approved tools.
8. Finally, the PM has been informed that there are significant budget cuts facing the organization this year. It will affect PCOMS staffing, hardware maintenance, and support contracts.

Task 1: Areas of Concern (Vulnerabilities) Likelihood, Impact and Risk

During the meeting, the Program Manager hands out the Vulnerabilities Analysis worksheets as shown below. As you can see, some of the weaknesses are provided. This information would represent some of what you would have already done as preliminary work and can be used as types of information you would have gathered. *(Note that several questions you should be considering have been included. Asking these questions will help you in your decision-making as you implement and assess the controls.)*

Instructions

1. Read the Program Manager's "Areas of Concern". Compare his comments with the threat events and potential vulnerabilities listed on the relevant Vulnerabilities Analysis Worksheet for the category assigned to your team.
2. In the Vulnerabilities Analysis worksheet, the Likelihood score has already been provided. Determine the Impact and Risk Score for each threat event/vulnerability.
3. Create a summary on the Areas of Concern Worksheet based on:
 - a. Four areas of concern - medium to extreme risk. (potential vulnerabilities)
 - b. Risk Scores for each concern/vulnerability. (Likelihood x Impact)
4. Select the vulnerability with the highest Risk Score.
5. Place the highest score in the Summary Risk Score Report.
6. Be prepared to conduct an informal report to the class based on your findings.

Example "Improper Handling":

1. Refer to the "Data" worksheet example at the Threat Event "Disclosure/Improper Handling".
 - a. A likelihood of "H" has been determined for the threat event based on the Program Manager's comments and the potential vulnerability. The value for "H" from the Likelihood Score Table (pg. 10) is "4".

b. Next, impact to the system has been determined as “Damaging” and a score of “3” assigned from the Impact ScoreTable.

2. The impact is rated as “Damaging” because if remote users handle sensitive data improperly, those who do not have a “need to know” may access it. The result could be damage to the organization mission.

3. The vulnerability or weakness is the lack of knowledge regarding protection levels due to ineffective INFOSEC Awareness training.

4. Refer to the tables below to obtain values for Likelihood “High” (value = 4) and Impact “Damaging” (value = 3). The risk score for this example is therefore 12 (Lx I).

Resources

- Worksheet 1: Vulnerabilities Analysis by Areas of Concern
- Likelihood Score, Impact Score and Risk Score Tables (Next page)

Likelihood Score Table

LIKELIHOOD SCORE		
Negligible	Is unlikely to occur < 1% chance	0
Very Low	May occur only in exceptional circumstances 1% - 3% chance	1
Low	Is unlikely, but could occur > 3% - 10% chance	2
Medium	Might occur > 10% - 50% chance	3
High	Will probably occur > 50% - 90% chance	4
Very High	Is expected to occur > 90% chance	5

Impact Score Table

IMPACT SCORE		
Insignificant	No impact	0
Minor	No extra effort required to repair	1
Significant	Tangible harm, extra effort required to repair	2
Damaging	<ul style="list-style-type: none"> Significant expenditure of resources required Damage to reputation and confidence 	3
Serious	<ul style="list-style-type: none"> Extended outage and / or loss of connectivity Compromise of large amounts of data or services 	4
Grave	<ul style="list-style-type: none"> Permanent shutdown Complete compromise 	5

Risk Score Key

RISK SCORE	
0	NIL
1 - 3	Low
4 - 7	Medium
8 - 14	High
15 - 19	Critical
20 - 30	Extreme

Data Vulnerabilities Worksheet

Threat (Event)	Potential Vulnerabilities in: Data	L	I	R
EXAMPLE: Disclosure/ Improper handling	EXAMPLE: Unknown protection levels (Specific weakness: Ineffective INFOSEC Awareness) <ul style="list-style-type: none"> Do personnel know about the classification scheme and protection levels? 	H-4	3	12
Data Spillage	Inadvertent exposure of sensitive information <ul style="list-style-type: none"> Can unencrypted sensitive data be compromised? 	H		
Intentional disclosure	Lack of employee non-disclosure agreements <ul style="list-style-type: none"> Is there any protection against employee disclosure? 	H		
Unintentional security breach	Inadequate security awareness <ul style="list-style-type: none"> Is there an effective Information Security Awareness program? 	H		
Asset misuse	Lack of understanding; Acceptable Use Policy <ul style="list-style-type: none"> Is proper conduct documented and understood? 	H		
Social engineering	Inadequate security awareness <ul style="list-style-type: none"> What is the potential for social engineering 	H		
Authentication Theft	Exposed passwords <ul style="list-style-type: none"> What is the potential for compromising user accounts? 	M		
Eavesdropping	Overhear conversations Open office / cube farms <ul style="list-style-type: none"> Can controlled conversations be overheard? 	VH		
Exposure	Unattended screen data Shoulder surfing <ul style="list-style-type: none"> Can data be easily exposed by shoulder surfing? 	VH		
Unattended Reproduction	Printer/Copier <ul style="list-style-type: none"> Are controlled documents left unattended at printers or copiers? 	M		

Applications Vulnerabilities Worksheet

Threat (Event)	Potential Vulnerabilities in Applications	L	I	R
Uncontrolled introduction/ Unauthorized apps	Inadequate configuration control (Specific Weakness: configuration changes) <ul style="list-style-type: none"> Is there a configuration control process to approve and track changes or additions? 	H		
Contractor Application Development	Inadequate application audits (Specific weakness: Lack of baselines) <ul style="list-style-type: none"> Is there baseline application documentation? 	M		
	Inadequate application audits (Specific weakness: Test Data) <ul style="list-style-type: none"> Is there adequate protection of test data? 	M		
	Inadequate application audits (Specific weakness: Source Library) <ul style="list-style-type: none"> Is there authorized access control to program source library? 	M		
Failure/ App shutdown	Inadequate revision control (Specific weakness: No discipline) <ul style="list-style-type: none"> Is there an effective revision control process? 	M		
Disruption	App accessible to outsiders (Specific weakness: Unattended terminals) <ul style="list-style-type: none"> Unattended terminals remain logged on? 	H		
	Inadequate documentation (Specific weakness: Configurations) <ul style="list-style-type: none"> Is there a documentation process for app disruptions? 	H		
	Inadequate bug/update tracking (Specific weakness: No role assigned) <ul style="list-style-type: none"> Is there a tracking process for updates and unauthorized access? 	H		
Uncontrolled exposure	3rd party non-disclosure agreements (Specific weakness: Contract programmers) <ul style="list-style-type: none"> Do contract programmers have access to controlled data and do they have contractual non-disclosure agreements? 	M		

Server Vulnerabilities Worksheet

Threat (Event)	Potential Vulnerabilities in Servers	L	I	R
Uncontrolled introduction/ Unauthorized servers	Inadequate configuration control (Specific weakness: No configuration control process to approve and track new additions or new servers) • Is there a configuration process for new servers?	H		
Failure/ Hardware malfunction	Inadequate spare parts (Specific weakness: Inadequate service contracts or spare parts) • Is there a contract in place for hardware maintenance?	M		
	Inadequate preventive (Specific weakness: Inadequate training) • Are onsite staff able to repair and maintain?	M		
OS malfunction	Adequate tools training • Does the staff have adequate training to run tools?	M		
	Are OS's patched and updated? • Does the staff perform adequate bug/update tracking?	H		
	Are onsite staff able to administer? • Does the staff have proper authority to administer tools?	H		
OS disruption	OS accessible to outsiders • Are unattended administrator workstations logged in?	M		
Accounts	Inadequate account authentication • Do administrators have 2-factor authentication?	M		
Administrative compromise	Inadequate accountability (Specific weakness: Tracking of admin logons) • Are all admin logons properly logged and audited?	H		

Infrastructure Vulnerabilities Worksheet

Threat (Event)	Potential Vulnerabilities in Infrastructure	L	I	R
Flood	Location in floodplain <ul style="list-style-type: none"> Are there flood walls in place to protect the facility? 	VL		
Storm	Location <ul style="list-style-type: none"> Any location-based storm problems such as hurricane or tornado alley? 	H		
Facility fire	Inadequate fire protection system <ul style="list-style-type: none"> Is there a fire code and does the facility meet it? 	H		
	No evacuation security procedures <ul style="list-style-type: none"> Is there an effective evacuation procedure with INFOSEC input? 	H		
	Fire department response time <ul style="list-style-type: none"> Is Fire Dept. response time a concern? 	H		
	Lack of control over neighboring floors <ul style="list-style-type: none"> Do other building tenants exacerbate building fire potential 	H		
Services loss	<ul style="list-style-type: none"> Are there emergency supplies on-hand for simple contingencies 	M		
Power failure	Inadequate redundancy <ul style="list-style-type: none"> Are there generators and has fuel supply, and testing been considered? 	H		
	UPS <ul style="list-style-type: none"> Are UPS's sufficiently sized, tested, batteries maintained? 	H		

Roles and Responsibilities Vulnerabilities Worksheet

Threat (Event)	Potential Vulnerabilities in Roles and Responsibilities (System Administrators)	L	I	R
Intentional collusion	Inadequate job rotation; inadequate checks and balances <ul style="list-style-type: none"> Can mischief be performed? 	M		
	<ul style="list-style-type: none"> Co-mingling of roles; inadequate checks and balances 	M		
Temporary Absence or Removal from role	Lack of cross training <ul style="list-style-type: none"> Is this role cross trained? 	H		
	Inadequate documentation <ul style="list-style-type: none"> Is there documentation sufficient to allow another to fill this role on a temporary basis? 	M		
Long term /permanent	Inadequate staffing budget No qualified applicants; skills shortage <ul style="list-style-type: none"> Is this role difficult to fill? 	M		
Accidental error	Insufficient employee training <ul style="list-style-type: none"> What IT or functional role-based training is lacking? 	H		
Intentional error	Malicious intent <ul style="list-style-type: none"> Is there sufficient compartmentalization in roles? 	M		
Poor role performance	Misunderstanding of responsibilities <ul style="list-style-type: none"> Do written job descriptions exist incorporating role responsibilities? 	M		
Physical	ID cards <ul style="list-style-type: none"> What is the potential to physically assume this role identity? 	L		

Task 2: Identify Medium to Extreme Risks (Areas of Concern Worksheet)

Using the results of your group's Risk Analysis by Areas of Concern (Vulnerabilities), list these vulnerabilities in the Areas of Concern worksheet below. Prepare a brief statement that describes the risk concern. This type of analysis will assist in prioritizing the implementation of controls.

RISK SCORE	AREA OF CONCERN VULNERABILITIES: DATA
RISK SCORE	AREA OF CONCERN VULNERABILITIES: APPLICATIONS
RISK SCORE	AREA OF CONCERN VULNERABILITIES: SERVERS

RISK SCORE	AREA OF CONCERN VULNERABILITIES: INFRASTRUCTURE
RISK SCORE	AREA OF CONCERN VULNERABILITIES: ROLES AND RESPONSIBILITIES

Task 3: Prepare a Summary Risk Score Report for Management

One of the key factors in managing risk is determining a way to convey the data in a meaningful form to management. For this activity, you are to determine the overall risk of the area of concern your team has been assigned. Using the results of the previous tasks, identify risks with the highest values for each asset category. Use the table below to generate a summary with risk scores that would help convey the risk.

Worksheet 3: Summary Risk Score Report						
Areas of Concern Summary Statistics	Extreme	Critical	High	Medium	Low	NIL
1. Data						
2. Applications						
3. Servers						
4. Infrastructure						
5. Roles and Responsibilities						

Walkthrough Analysis of PCOMS Boundary and Information Types

Information Types Based on the System Description

The PCOMS Program Manager has decided that the application requires special management and security oversight due to the sensitivity of the information resident on the system. Due to this determination, PCOMS has been designated a Major Application for the purposes of the Security Assessment and Authorization (SA&A).

The Photography Adjustment and Management (PAM) Act of 1993 established photography collection programs and associated monitoring and reporting mechanisms designed to enhance photographic capabilities for the US government.

The **Geospatial Operations Organization (GOO)**, an agency of the **Department of Ultra Diehards (DUD)**, has been involved in the acquisition, use, and distribution of aerial photography for more than 35 years for DUD and other authorized users. The mission of the GOO is to provide rectified and annotated aerial and ground photographs for accurately measuring and repairing DUD Reserves and facilities. The PCOMS supports the GOO mission through the acquisition, collection, rectification, storage, and distribution of imagery data.

The Aerial Photography Program Management Office (AP2MO), a division of GOO, provides imagery acquisition, rectification, inspection, distribution and archiving services for GOO, DUD, authorized federal and state agencies, and other approved users and associates through the operations and management of the PCOMS. PCOMS end users, including those outside the DUD, are located nationally with secured web access (HTTPS) to the PCOMS application.

GOO also has the mission of ensuring installation maintenance which includes maintaining and operating public lands, buildings, monuments, and surrounding property. This also includes activities devoted to ensuring the preservation of land, water, wildlife, and natural resources. It includes the sustainable stewardship of natural resources on federally owned/controlled lands for commercial use (mineral mining, grazing, forestry, fishing, etc.).

Information Types Based on the PCOMS Subsystem Applications

As part of the PCOMS, the **Photography Consolidated Management Sub-system (PCMS)** automates AP2MO dashboard capabilities. The dashboard provides GOO senior management high-level insight into DUD Reserve management programs and monitoring for PAM Act requirements.

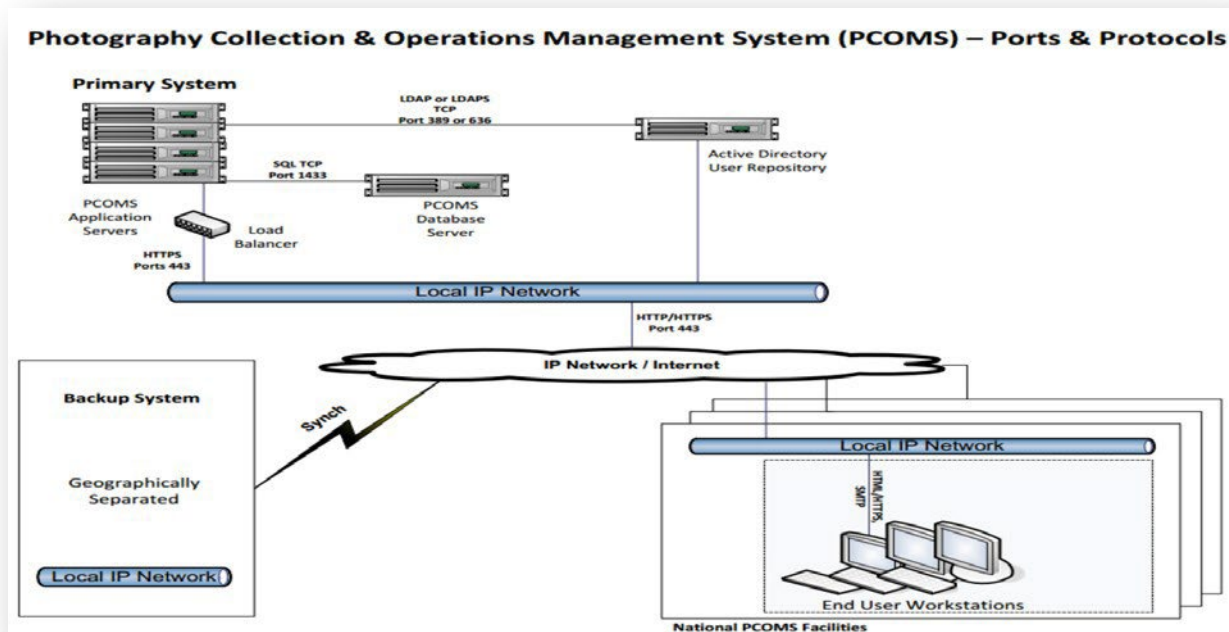
Additionally, the **Geospatial Management Office Subsystem (GMOS)**, a PCOMS sub-system, provides access to the accurate, authoritative, trusted source of imagery and other geospatial datasets by GOO agency users, such as the Service Center Universal Manager (SCUM) subscribers.

As stated earlier in the risk assessment activity, the PCOMS is hosted in the Hosting and Operations and Services Division (HOSD) mixed Linux and Microsoft Windows data center environment. As part of the hosting agreement, HOSD provides Enterprise Active Directory (EAD), security, network, and monitoring services. AP2MO management, through AP2MO system and database administrators, is responsible for all hardware, operating systems, databases, installation, administration, authorization, purchasing and maintenance of the PCOMS application and all sub-components.

PCOMS is a tenant of the RITOF facility. The RITOF Facility is responsible for the building environment (e.g. HVAC, electrical, etc.) and RSOC and ROTS (Telecommunications – LAN, telephony) (Both are separate organizations within RITOF)

This PCOMS diagram depicts the system and the interconnection with other systems. It would include the kind of data that is processed/transferred/stored.

You need detail on what information is processed on the system because the categorization of the system determines the implementation of the controls.



CATEGORIZE

Activity 2: Determine Boundary and Categorization for the LIMBO System

For this activity, familiarize yourself with the Location Inventory Management Baseline Operations (LIMBO) system by reading the system description below. Then review and answer the questions following the description to determine the system boundary.

In addition, you will propose information types that are processed, stored, or transmitted by the LIMBO system. Refer to NIST SP 800-60 V2 and the BAI Reference Guide (NIST SP 800-60 V2 Information Types) to identify LIMBO information types. Be prepared to report your proposed information types along with a proposed rationale for each one recommended.

LIMBO Information System Type

The Location Inventory Management Baseline Operations (LIMBO) system owner has determined that the application requires special management and security oversight because of the sensitivity of the information resident on the system. Due to this determination, the LIMBO system has been designated a Major Application for the purposes of the Security Assessment and Authorization (SA&A).

LIMBO System Description

The LIMBO system supports the enactment of Department of Ultra Diehards (DUD) and US government policies and the Warehouse Management Act (WMA) of 1921 to acquire, store, and distribute paper product inventories to support the individual DUD facilities and agencies. This is accomplished through an integrated online and batch database system which controls and accounts for the acquisition, storage, inventory, product specifics, and distribution of paper products. The system, through subsystems, provides dashboard reports on the acquisition, storage, and disposition of all DUD- owned paper inventories.

The system accepts bid packages and associated proprietary information from potential vendors and allows bidders secure access to individual sensitive bid status and disposition information on each of their proposals and bid selection actions. The LIMBO system is a customized version of a commercial off the shelf (COTS) product. It is owned and operated by the **Paperwork Reduction and Elimination Agency (PREA)** of the Department of Ultra Diehards (DUD).

The paper products managed by the LIMBO system are for use by DUD agencies. All DUD LIMBO system employee and contractor end users are located at facilities within the geographic region for which the individual DUD Reserve LIMBO system is responsible and access the system via secured web access (HTTPS) over the DUD network. Paper product

vendors also access the LIMBO system via the secured web access (HTTPS) over the internet and DUD network.

The PREA, through the LIMBO system, focuses on contracting to small and disadvantaged businesses and works closely with the Small Business Administration (SBA) to identify targeted businesses.

The LIMBO system major sub-functions include:

- Inventory acquisition, control, storage, and distribution
- Paper product catalogs
- Loading, Order Control, and Settlements
- Invoice verification and electronic payment

LIMBO Subsystems:

The **Paper Commodity Inventory Subsystem (PCIS)** is a subset of business functions associated with the LIMBO system that supports the enactment of DUD and US government policies and the Warehouse Management Act (WMA). PCIS entails the special aspects of the **Printer Paper Inventories Management Sub-system (PPIMS)** and handles unique characteristics of the printer paper inventories such as paper size, color, weight, etc.

The **Paper Marketing Certificate Subsystem (PMCS)** authorizes payment of invoices for electronic payments to local suppliers to keep prices competitive under the Extra Long Staple Paper Program and supports the Paper Adjustment Assistance Program of the WMA. Since they are small businesses, some paper product vendors utilize their Social Security Numbers (SSN) as their Employer Identification Numbers (EIN) in the vendor profiles.

LIMBO Technical Overview

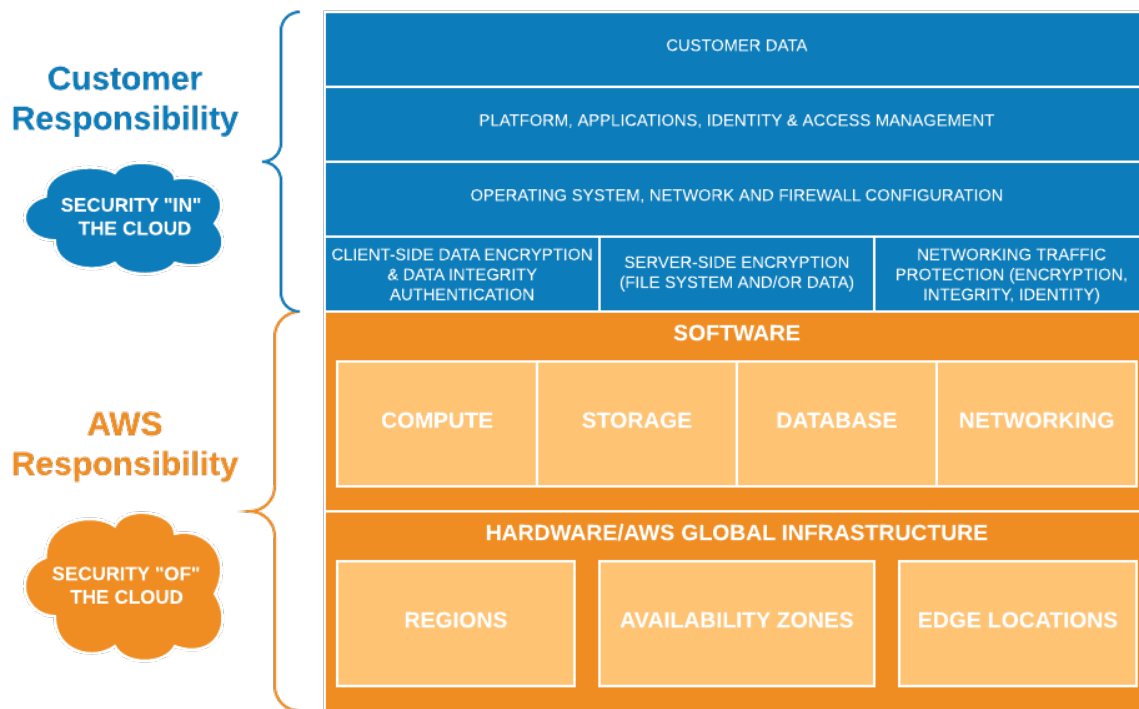
The PREA system administrators install, administer, and maintain all application, operating systems, and database components for the LIMBO system as part of an Infrastructure as a Service (IAAS) cloud model utilizing the Amazon Web Services (AWS) GovCloud. Due to the fact that LIMBO collects privacy information, the cloud solution is deployed at an Impact Level 4 (IL4). The AWS GovCloud provides the computing infrastructure, physical and virtual machines and other resources such as file-based storage, load balancers, IP addresses, etc. It provides secure access to LIMBO system vendors to submit bid packages and associated proprietary information as well as invoices for electronic payments. For IAAS offerings, the Mission Owner (PREA) is responsible for administration of:

- Operating systems
- Applications
- Data in Transit
- Data at Rest
- Databases
- Credentials to private keys

- Adhering to DoD Policies and Configurations (i.e., STIGs)
- Vulnerability Compliance Reporting

The following Cloud Service Provider (CSP) Shared Responsibility Model depicts LIMBO (Customer) and CSP responsibilities.

Table 1: CSP Shared Responsibility Model



Answer the following questions to determine the LIMBO system boundary.

- Who owns the system?
- Who operates the system?
- What are the inputs for the system?
- What actions does the system perform?
- What is the output?
- What are the major subsystems?
- What is the system user base?

Categorize the LIMBO System

Instructions: Read through the description for the LIMBO system to respond to the following:

- 1) Identify any laws, directives, policies, or guidance that this system needs to follow when categorizing the system.
- 2) What is the function and sub-functions of the system?
- 3) Identify the system type.
- 4) Using the NIST SP 800-60, Volume 2, and the NIST SP 800-60 Table of Contents in the BAI Reference Handout (Appendices C and D), what Information Types should potentially be included for the LIMBO system? Select a minimum of four Information Types.
- 5) What is the overall categorization of the LIMBO system?

Categorize Documentation:

In which documents would you summarize the results of the information you gathered during the Categorize step?

SELECT

Activity 3: Identify PCOMS Security Control Requirements

For this activity, return to your Risk Assessment teams. Each team will revisit the Areas of Concern Summary proposed during the Risk Assessment (Activity 1) to identify security control families that may apply to those areas of concern and start selecting security controls to mitigate system risks. Return to your responses in the Summary Chart – Areas of Concern Worksheet - from the Risk Assessment Activity to find the four risks your team identified.

- For your group Area of Concern, find security control families that provide security capabilities that address the concerns of the Program Manager.
- Refer to the BAI Reference Guide or the NIST SP 800-53 control catalog. Be prepared to propose at least one security control for each risk and provide your recommendation for improvement.
- Plan to conduct a report to the class based on your team's recommendations.
- Collect your answers in the "Areas of Risk Concern" tables below.

Security Control Families (NIST SP 800-53 R4)

AC	Access Control	MP	Media Protection
AT	Awareness and Training	PE	Physical and Environmental Protection
AU	Audit and Accountability	PL	Planning
CA	Security Assessment and Authorization	PS	Personnel Security
CM	Configuration Management	RA	Risk Assessment
CP	Contingency Planning	SA	Systems and Services Acquisition
IA	Identification and Authentication	SC	System and Communications Protection
IR	Incident Response	SI	System and Information Integrity
MA	Maintenance	PM	Program Management

Security Control Families (NIST SP 800-53 R5)

ID	FAMILY	ID	FAMILY
AC	Access Control	PE	Physical and Environmental Protection
AT	Awareness and Training	PL	Planning
AU	Audit and Accountability	PM	Program Management
CA	Assessment, Authorization, and Monitoring	PS	Personnel Security
CM	Configuration Management	PT	PII Processing and Transparency
CP	Contingency Planning	RA	Risk Assessment
IA	Identification and Authentication	SA	System and Services Acquisition
IR	Incident Response	SC	System and Communications Protection
MA	Maintenance	SI	System and Information Integrity
MP	Media Protection	SR	Supply Chain Risk Management

AREAS of CONCERN		
DATA		
Risk: Recommendation:	Control No:	Control Title:
Risk: Recommendation:	Control No:	Control Title:
Risk: Recommendation:	Control No:	Control Title:
Risk: Recommendation:	Control No:	Control Title:
APPLICATIONS		
Risk: Recommendation:	Control No:	Control Title:
Risk: Recommendation:	Control No:	Control Title:
Risk: Recommendation:	Control No:	Control Title:
Risk: Recommendation:	Control No:	Control Title:

SERVERS

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

PHYSICAL INFRASTRUCTURE

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

ROLES AND RESPONSIBILITIES

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

Risk: Control No: Control Title:
Recommendation:

Activity 4: Allocate PCOMS Security Controls

There are three types of security controls for information systems that can be employed by an organization:

- a. *system-specific controls* (i.e., controls that provide a security capability for a particular information system only)
- b. *common controls* (i.e., controls that provide a security capability for multiple information systems)
- c. *hybrid controls* (i.e., controls that have both system-specific and common requirements).

Task 1: Allocate Security Controls - Propose Common/Inherited, Hybrid or System Specific Controls

Review each of the controls below. Determine whether they are System Specific, Common (Inheritable), or Hybrid controls for the PCOMS system:

Note: Additional Control Discussions are found in the BAI Reference Guide,

NIST SP 800-53 R5 - Security Control Catalog – Excerpts of Controls

Control	Control Description	System Specific (S) Common (C) Hybrid (H)
AC-4 – Information Flow Enforcement	Enforce approved authorizations for controlling the flow of information within the system and between connected systems based on [Assignment: <i>organization-defined information flow control policies</i>].	
AC-9 – Previous Logon Notification	Notify the user, upon successful logon to the system, of the date and time of the last logon.	
AT-2 - Literacy Training and Awareness	a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors): 1. As part of initial training for new users and [Assignment: <i>organization-defined frequency</i>] thereafter; and 2. When required by system changes or following [Assignment: <i>organization-defined events</i>]	

Control	Control Description	System Specific (S) Common (C) Hybrid (H)
AU-5 – Response to Audit Logging Process Failures	<p>a. Alert [Assignment: organization-defined personnel or roles] within [Assignment: organization-defined time period] in the event of an audit logging process failure; and</p> <p>b. Take the following additional actions: [Assignment: organization-defined actions to be taken (e.g., shut down information system, overwrite oldest audit records, stop generating audit records)].</p>	
CA-5 – Plan of Action and Milestones	<p>a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and</p> <p>b. Update existing plan of action and milestones [Assignment: organization-defined frequency] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.</p>	
CP-7 – Alternate Processing Site	<p>a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: organization-defined system operations] for essential mission and business functions within [Assignment: organization-defined time period consistent with recovery time and recovery point objectives] when the primary processing capabilities are unavailable.</p> <p>b. Make available at the alternate processing site; the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and</p> <p>c. Provide controls at the alternate processing site that are equivalent to those at the primary site.</p>	
IR-4 – Incident Handling	<p>a. Implement an incident handling capability for incidents that is consistent with the incident response plan and includes preparation, detection and analysis, containment, eradication, and recovery.</p> <p>b. Coordinate incident handling activities with contingency planning activities.</p> <p>c. Incorporate lessons learned from ongoing incident handling activities into incident response procedures, training, and testing, and implement the resulting changes accordingly.</p>	.

Control	Control Description	System Specific (S) Common (C) Hybrid (H)
PE-17 – Alternate Work Site	<p>a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees.</p> <p>b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls].</p> <p>c. Assess the effectiveness of controls at alternate work sites; and</p> <p>d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.</p>	
PS-2 – Position Risk Designation	<p>a. Assign a risk designation to all organizational positions.</p> <p>b. Establish screening criteria for individuals filling those positions; and</p> <p>c. Review and update position risk designations [Assignment: organization-defined frequency].</p>	
RA-2 – Security Categorization	<p>a. Categorize the system and information it processes, stores, and transmits.</p> <p>b. Document the security categorization results, including supporting rationale, in the security plan for the system; and</p> <p>c. Verify that the authorizing official or authorizing official designated representative reviews and approves the security categorization decision.</p>	

Control	Control Description	System Specific (S) Common (C) Hybrid (H)
SA-5 – System Documentation	<p>a. Obtain or develop administrator documentation for the system, system component, or system service that describes:</p> <ol style="list-style-type: none"> 1. Secure configuration, installation, and operation of the system, component, or service. 2. Effective use and maintenance of security and privacy functions and mechanisms; and 3. Known vulnerabilities regarding configuration and use of administrative or privileged functions. <p>b. Obtain or develop user documentation for the system, system component, or system service that describes:</p> <ol style="list-style-type: none"> 1. User-accessible security and privacy functions and mechanisms and how to effectively use those functions and mechanisms. 2. Methods for user interaction, which enables individuals to use the system, component, or service in a more secure manner and protect individual privacy; and 3. User responsibilities in maintaining the security of the system, component, or service and privacy of individuals. <p>c. Document attempts to obtain system, system component, or system service documentation when such documentation is either unavailable or nonexistent and take <i>[Assignment: organization-defined actions]</i> in response; and</p> <p>d. Distribute documentation to <i>[Assignment: organization-defined personnel or roles]</i>.</p>	
SC-2 – Separation of System and User Functionality	Separate user functionality, including user interface services, from system management functionality.	
SR-2 - Supply Chain Risk Management Plan	<ol style="list-style-type: none"> a. Develop a plan for managing supply chain risks associated with the research and development, design, manufacturing, acquisition, delivery, integration, operations and maintenance, and disposal of the following systems, system components or system services: <i>[Assignment: organization-defined systems, system components, or system services]</i>. b. Review and update the supply chain risk management plan <i>[Assignment: organization defined frequency]</i> or as required, to address threat, organizational or environmental changes; and c. Protect the supply chain risk management plan from unauthorized disclosure and modification. 	

Activity 4 – Additional Controls

Control	Control Description	System Specific (S) Common (C) Hybrid (H)
AC-2(5) – Account Management: Inactivity Logout	Require that users log out when <i>[Assignment: organization-defined time period of expected inactivity or description of when to log out]</i> .	
AC-8 – System Use Notification	<p>a. Display <i>[Assignment: organization-defined system uses notification message or banner]</i> to users before granting access to the system that provides privacy and security notices consistent with applicable laws, executive orders, directives, regulations, policies, standards, and guidelines and state that:</p> <ol style="list-style-type: none"> 1. Users are accessing a U.S. Government system. 2. System usage may be monitored, recorded, and subject to audit. 3. Unauthorized use of the system is prohibited and subject to criminal and civil penalties; and 4. Use of the system indicates consent to monitoring and recording. <p>b. Retain the notification message or banner on the screen until users acknowledge the usage conditions and take explicit actions to log on to or further access the system; and</p> <p>c. For publicly accessible systems:</p> <ol style="list-style-type: none"> 1. Display system use information <i>[Assignment: organization-defined conditions]</i>, before granting further access to the publicly accessible system. 2. Display references, if any, to monitoring, recording, or auditing that are consistent with privacy accommodations for such systems that generally prohibit those activities; and 3. Include a description of the authorized uses of the system. 	
CA-3 – Information Exchange	<p>a. Approve and manage the exchange of information between the system and other systems using <i>[Selection (one or more): interconnection security agreements; information exchange security agreements; memoranda of understanding or agreement; service level agreements. user agreements; nondisclosure agreements; [Assignment: organization-defined type of agreement]]</i>.</p> <p>b. Document, as part of each exchange agreement, the interface characteristics, security and privacy requirements, controls, and responsibilities for each system, and the impact level of the information communicated.</p>	

MP-6 – Media Sanitization	<p>a. Sanitize [<i>Assignment: organization-defined system media</i>] prior to disposal, release out of organizational control, or release for reuse using [<i>Assignment: organization-defined sanitization techniques and procedures</i>]; and</p> <p>b. Employ sanitization mechanisms with strength and integrity commensurate with the security category or classification of the information.</p>	
PE-3(1) – Physical Access Control: System Access	Enforce physical access authorizations to the system in addition to the physical access controls for the facility at [<i>Assignment: organization-defined physical spaces containing one or more components of the system</i>].	
PE-12 – Emergency Lighting	Employ and maintain automatic emergency lighting for the system that activates in the event of a power outage or disruption and that covers emergency exits and evacuation routes within the facility.	
PS-6 – Access Agreements	<p>a. Develop and document access agreements for organizational systems.</p> <p>b. Review and update the access agreements [<i>Assignment: organization-defined frequency</i>]; and</p> <p>c. Verify that individuals requiring access to organizational information and systems:</p> <ol style="list-style-type: none"> 1. Sign appropriate access agreements prior to being granted access; and 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [<i>Assignment: organization-defined frequency</i>]. 	

Task 2: Allocate Security Controls - Assessment

- 1) The Geospatial Operations Organization (GOO) with concurrence from the DUDCIO, has determined that PCOMS has a low priority for the Availability security objective. Therefore, the PCOMS Program Manager has directed that the requirements for Control Enhancement CP-2(1), Contingency Plan | Coordinate with Related Plans, be downgraded to Low from the CNSSI 1253 Moderate baseline Availability selection. This is an example of:
 - a. Applying Compensating Controls
 - b. Applying Scoping Guidance
 - c. Organizational Parameterization
 - d. Supplementing the Control Baseline
- 2) PCOMS does not have the capability to utilize Voice of Internet Protocol (VoIP) services. Consequently, the Information System Security Officer (ISSO) has determined that the SC-19, Voice over Internet Protocol, control is not applicable to the system. This is an example of:
 - a. Tailoring the Control Baseline
 - b. Applying Compensating Controls
 - c. Organizational Parameterization
 - d. Supplementing the Control Baseline
- 3) PCOMS has been configured to disconnect or disable remote access connections, as needed, within 20 minutes of notification for the system. This is an example of:
 - a. Tailoring the Control Baseline
 - b. Applying Compensating Controls
 - c. Organizational Parameterization
 - d. Supplementing the Control Baseline
- 4) The Information System Security Engineer (ISSE) and Information System Security Officer (ISSO) have received approval to implement AC-24, Access Control Decisions. This is an example of:
 - a. Tailoring the Control Baseline
 - b. Applying Compensating Controls
 - c. Organizational Parameterization
 - d. Supplementing the Control Baseline

- 5) One of the Universal Service Centers has a web access component that supplies data to PCOMS but is configured to allow password resets annually for supplier access to their system. Consequently, the PCOMS Information System Security Officer (ISSO) has the RITOF Security Operations Center review all web access account logs for unusual activity every 15 days. This is an example of:
- a. Tailoring the Control Baseline
 - b. Applying Compensating Controls
 - c. Organizational Parameterization
 - d. Supplementing the Control Baseline

IMPLEMENTATION/ASSESS

Activity 5: IMPLEMENT/ASSESS/Continuous Monitoring Activity

Instructions

For the listed security controls below, develop an implementation statement and then identify the assessment methods (Examine, Interview & Test) and the evidence that you would collect for each assessment.

Follow with a Continuous Monitoring Plan.

- a) How would you perform the monitoring activity or activities?
- b) What frequency will you assign for performance and review or test of the monitoring activity or activities?
- c) Who performs the monitoring activity – a job position or organization?
- d) What are the expected results? Are you using a metric? How do you report and/or track issues that result from the monitoring activity?
- e) In what document or documents do you record the completion of the monitoring activity?

Note: Additional Control Discussions are found in the BAI Reference Guide,

NIST SP 800-53 R5 - Security Control Catalog – Excerpts of Controls

AT-2 LITERACY TRAINING AND AWARENESS

Control:

- a. Provide security and privacy literacy training to system users (including managers, senior executives, and contractors):
 1. As part of initial training for new users and [*Assignment: organization-defined frequency - Annually*] thereafter; and
 2. When required by system changes or following [*Assignment: organization-defined events*]

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

CA-5 PLAN OF ACTION AND MILESTONES

Control:

- a. Develop a plan of action and milestones for the system to document the planned remediation actions of the organization to correct weaknesses or deficiencies noted during the assessment of the controls and to reduce or eliminate known vulnerabilities in the system; and
- b. Update existing plan of action and milestones [*Assignment: organization-defined frequency*] based on the findings from control assessments, independent audits or reviews, and continuous monitoring activities.

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization	

performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

IR-9 INFORMATION SPILLAGE RESPONSE

Control: Respond to information spills by:

- a. Assigning [*Assignment: organization-defined personnel or roles*] with responsibility for responding to information spills.
- b. Identifying the specific information involved in the system contamination.
- c. Alerting [*Assignment: organization-defined personnel or roles*] of the information spill using a method of communication not associated with the spill.
- d. Isolating the contaminated system or system component.
- e. Eradicating the information from the contaminated system or component.
- f. Identifying other systems or system components that may have been subsequently contaminated; and
- g. Performing the following additional actions: [*Assignment: organization-defined actions*].

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

CP-7 ALTERNATE PROCESSING SITE

Control:

- a. Establish an alternate processing site, including necessary agreements to permit the transfer and resumption of [Assignment: *organization-defined system operations*] for essential mission and business functions within [Assignment: *organization-defined time period consistent with recovery time and recovery point objectives*] when the primary processing capabilities are unavailable.
- b. Make available at the alternate processing site; the equipment and supplies required to transfer and resume operations or put contracts in place to support delivery to the site within the organization-defined time period for transfer and resumption; and
- c. Provide controls at the alternate processing site that are equivalent to those at the primary site.

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

CP-9 SYSTEM BACKUP

Control:

- a. Conduct backups of user-level information contained in *[Assignment: organization-defined system components]* *[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]*.
- b. Conduct backups of system-level information contained in the system *[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]*.
- c. Conduct backups of system documentation, including security- and privacy-related documentation *[Assignment: organization-defined frequency consistent with recovery time and recovery point objectives]*; and
- d. Protect the confidentiality, integrity, and availability of backup information.

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

PS-6 ACCESS AGREEMENTS

Control:

- a. Develop and document access agreements for organizational systems.
- b. Review and update the access agreements [*Assignment: organization-defined frequency*]; and
- c. Verify that individuals requiring access to organizational information and systems:
 - 1. Sign appropriate access agreements prior to being granted access; and
 - 2. Re-sign access agreements to maintain access to organizational systems when access agreements have been updated or [*Assignment: organization-defined frequency*].

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	

Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

CM-3 CONFIGURATION CHANGE CONTROL

Control:

- a. Determine and document the types of changes to the system that are configuration controlled.
- b. Review proposed configuration-controlled changes to the system and approve or disapprove such changes with explicit consideration for security and privacy impact analyses.
- c. Document configuration change decisions associated with the system.
- d. Implement approved configuration-controlled changes to the system.
- e. Retain records of configuration-controlled changes to the system for [*Assignment: organization-defined time period*].
- f. Monitor and review activities associated with configuration-controlled changes to the system; and
- g. Coordinate and provide oversight for configuration change control activities through [*Assignment: organization-defined configuration change control element*] that convenes [*Selection (one or more): [Assignment: organization-defined frequency]*]; when [*Assignment: organization-defined configuration change conditions*]].

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring	

activity	
----------	--

AT-3 ROLE-BASED TRAINING

Control:

- a. Provide role-based security and privacy training to personnel with the following roles and responsibilities: *[Assignment: organization-defined roles and responsibilities]*:
 - 1. Before authorizing access to the system, information, or performing assigned duties, and *[Assignment: organization-defined frequency]* thereafter; and
 - 2. When required by system changes.
- b. Update role-based training content *[Assignment: organization-defined frequency]* and following *[Assignment: organization-defined events]*; and
- c. Incorporate lessons learned from internal or external security incidents or breaches into role-based training.

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

RA-5 VULNERABILITY MONITORING AND SCANNING

Control:

- a. Monitor and scan for vulnerabilities in the system and hosted applications [*Assignment: organization-defined frequency and/or randomly in accordance with organization-defined process*] and when new vulnerabilities potentially affecting the system are identified and reported.
- b. Employ vulnerability monitoring tools and techniques that facilitate interoperability among tools and automate parts of the vulnerability management process by using standards for:
 1. Enumerating platforms, software flaws, and improper configurations.
 2. Formatting checklists and test procedures; and
 3. Measuring vulnerability impact.
- c. Analyze vulnerability scan reports and results from vulnerability monitoring.

- d. Remediate legitimate vulnerabilities [*Assignment: organization-defined response times*] in accordance with an organizational assessment of risk.
- e. Share information obtained from the vulnerability monitoring process and control assessments with [*Assignment: organization-defined personnel or roles*] to help eliminate similar vulnerabilities in other systems; and
- f. Employ vulnerability monitoring tools that include the capability to readily update the vulnerabilities to be scanned.

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	

Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

CP-3 CONTINGENCY TRAINING

Control:

- a. Provide contingency training to system users consistent with assigned roles and responsibilities:
 - 1. Within [*Assignment: organization-defined time period*] of assuming a contingency role or responsibility.
 - 2. When required by system changes; and
 - 3. [*Assignment: organization-defined frequency*] thereafter; and
- b. Review and update contingency training content [*Assignment: organization-defined frequency*] and following [*Assignment: organization-defined events*].

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

PE-17 ALTERNATE WORK SITE

Control:

- a. Determine and document the [Assignment: organization-defined alternate work sites] allowed for use by employees.
- b. Employ the following controls at alternate work sites: [Assignment: organization-defined controls].
- c. Assess the effectiveness of controls at alternate work sites; and
- d. Provide a means for employees to communicate with information security and privacy personnel in case of incidents.

Implementation Statement:	
---------------------------	--

Examine	
Interview	
Test	

Performance Monitoring Activity	
---------------------------------	--

Recommended Frequency	
Individual or organization performing monitoring activity	
Expected Results	
Reporting (to whom)	
Tracking (resulting issues)	
Document that records completion of monitoring activity	

AUTHORIZE

Activity 6: Authorize Concepts Review Quiz

1. Which of the following roles can also serve as the Authorizing Official Designated Representative?
 - a) Information System Owner
 - b) Senior Information Security Officer(SISO)
 - c) Information System Security Manager (ISSM)
 - d) DoD Component Chief Information Officer(CIO)

2. Which of the following roles can approve the Security Plan?
 - a) Authorizing Official Designated Representative
 - b) Information System Security Manager (ISSM)
 - c) Senior Information Security Officer(SISO)
 - d) Information Owner

3. Which of the following roles has responsibility for signing the Authorization Decision Document?
 - a) Authorizing Official Designated Representative
 - b) Authorizing Official (AO)
 - c) Senior Information Security Officer(SISO)
 - d) Information System Owner

4. Which of the following roles has the responsibility of making the final risk determination for a system?
 - a) Authorizing Official Designated Representative (AODR)
 - b) DoD Component Chief Information Officer(CIO)
 - c) Senior Information Security Officer(SISO)
 - d) Information System Owner

5. Which of the following documents is NOT one of the key security authorization package documents?
 - a) The Plan of Action and Milestones (POAM)
 - b) The Security Plan (SP)
 - c) The Contingency Plan (CP)
 - d) The Security Assessment Report (SAR)

MONITOR

Activity 7: Maintaining Current Documentation during the Monitor Phase

For each of the “events” below, describe how each element of the RMF documentation package may (or may not) be affected. Also indicate any other significant effects on the authorization status of the system.

1. Contingency plan is successfully tested.

System Security Plan (SSP): _____

Security Assessment Report: _____

Plan of Action and Milestones (POA&M): _____

Other documents or effects (specify): _____

2. New software components are introduced as part of a system upgrade.

System Security Plan (SSP): _____

Security Assessment Report: _____

Plan of Action and Milestones (POA&M): _____

Other documents or effects (specify): _____

3. Annual IA Review is conducted, revealing several areas that are no longer fully compliant with assigned Security Controls.

System Security Plan (SSP): _____

Security Assessment Report: _____

Plan of Action and Milestones (POA&M): _____

Other documents or effects (specify): _____

4. The system is expanded to process a new information type.

System Security Plan (SSP): _____

Security Assessment Report: _____

Plan of Action and Milestones (POA&M): _____

Other documents or effects (specify): _____

5. The system is compromised or infected with malicious code.

System Security Plan (SSP): _____

Security Assessment Report: _____

Plan of Action and Milestones (POA&M): _____

Other documents or effects (specify): _____