A Monitor System in Data Redundancy in Information System

Varsha Soni[1]
[1]M. Tech (C.S.)Research Scholar
[1]Mewar University, Chittorgarh.

Abstract—The structure of a few of the Information Assurance (IA) processes currently being used in the United States government. In this paper, the general structure of the processes that are uncovered and used to create a Continuous Monitoring Process that can be used to create a tool to incorporate any process of similar structure. The paper defines a concept of continuous monitoring that attempts to create a process from the similar structure of several existing IA processes. The specific documents and procedures that differ among the processes can be incorporated to reuse scan results and manual checks that have already been conducted on an IS A proof-of-concept application is drafted to demonstrate the main aspects of the proposed tool. The possibilities and implications of the proof-of-concept application are explored, to develop a fully functional and automated version of the proposed Continuous Monitoring tool.

Keywords: DIACAP, common structure processes, Continuous monitoring process.

I. INTRODUCTION

In International relations, offensive advantage “means that it is easier to destroy the other’s army and take its territory than it is to defend one’s own” [1]. This can be translated in terms of cyber security to mean that it is easier to destroy the availability of the other’s information infrastructure and take its confidential information than it is to defend one’s own information infrastructure. Due to the fact that there is a clear offensive advantage in cyber warfare, it is important to ensure the security of information systems by having information assurance security controls in place and up-to-date. Information Assurance (IA) consists of the “measures that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation” [2]. Security controls are “the management, operational and technical controls (e.g., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information” [2]. The Federal Information Security Management Act (FISMA), include developing, documenting, and implementing an information security program and developing and maintaining an inventory of information systems under the control of the organization. The key requirements are to provide information security protections commensurate with the assessed risk and to compose annual reports on the effectiveness of the organization’s information security program [3].

The OMB Circular A-130, to review the security controls of their information systems to ensure that changes do not have a significant impact on security, IA controls continue to perform as intended, and security plans remain effective.

Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP) is how the OMB and FISMA requirements are met. The DIACAP ensures the risks associated with the information system (IS) are acceptable. It checks for compliance against the IA controls in the DoD Instruction 8500.2 Information Assurance (IA) Implementation. There are several IA Processes currently being used throughout the United States Government. Each department, such as the Department of Defense (DoD) and Department of State, has its own processes and internal standard operating procedures (SOPs). As a result, the same IA controls are checked in several processes, creating redundant work and wasting critical time. This redundancy can be reduced through continuous monitoring and reuse of automated scans and manual checks of the IA controls. Vulnerabilities to the IS can occur if IA controls are not performing as intended or new weaknesses to the system are not addressed. Without continuous monitoring, these vulnerabilities may go unnoticed until DIACAP re-certification which may be years away.

A. DIACAP

The DoDI 8510.01 establishes a process for DoD IA Certification and Accreditation that will authorize the operation of DoD information systems in accordance with FISMA [3], DoDD 8500.01 Information Assurance [7], DoDI 8500.2 Information Assurance Implementation, and DoDD 8100.1 Global Information Grid (GIG) Overarching Policy [8]. The process, shown in Figure 1 [9], consists of five activities that manage the implementation of IA controls and provide visibility of accreditation decisions regarding the operation of DoD information systems.

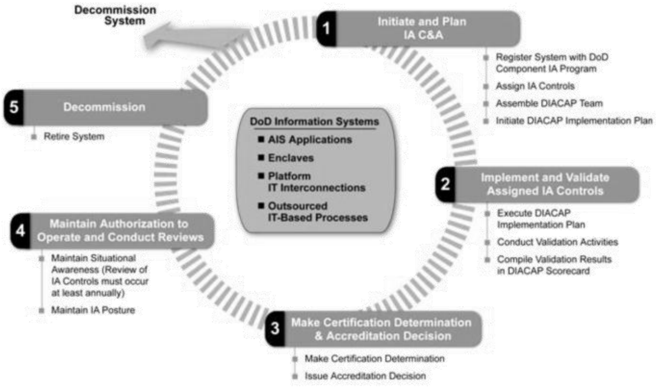

Decommission System
1 Initiate and Plan IA C&A
Register System with DoD Component IA Program
Assign IA Controls
Assemble DIACAP Team
Initiate DIACAP Implementation Plan
2 Implement and Validate Assigned IA Controls
Execute DIACAP Implementation Plan
Conduct Validation Activities
Compile Validation Results in DIACAP Scorecard
3 Make Certification Determination & Accreditation Decision
Make Certification Determination
Issue Accreditation Decision
4 Maintain Authorization to Operate and Conduct Reviews
Maintain Situational Awareness (Review of IA Controls must occur at least annually)
Maintain IA Posture
5 Decommission
Retire System
DoD Information Systems
AIS Applications
Enclaves
Platform IT Interconnections
Outsourced IT-Based Processes

Fig. 1: DIACAP Activities

B. *Initiate and Plan IA C&A*

It consists of preparatory actions for IA Certification and Accreditation. The baseline controls are adjusted to account for inherited, not applicable, and system-specific controls, and then compiled in the IA Control Implementation Plan. The Certification and Accreditation (C&A) Plan is formed From the IA Control Implementation Plan, and Validation Plan and Procedures. The DIACAP team is assembled to initiate the C&A Plan and the DIP.

C. Implement and Validate Assigned IA Controls

In the second activity, the DIP is executed and the assigned IA controls are implemented. Other systems are also checked in order to verify inherited controls. The implementation is documented and the DIP is updated. Validation activities are conducted to assess the effectiveness of the IA controls. The compliance status from the Validation Report is recorded in the DIACAP Scorecard, and, if corrective actions are necessary, the Plan of Actions and Milestones (POA&M) is prepared and/or updated.

D. Make Certification Determination and Accreditation Decision

The certification determination and accreditation decision takes place in activity three. The Certification Authority (CA) makes the certification determination based on the actual validation results, the impact codes and severity categories of non-compliant controls, expected exposure time, and costs of mitigation. The CA forwards either the Executive or Comprehensive Package to the Designated Accrediting Authority (DAA) to issue an accreditation decision. The DAA reviews the package and assesses the residual risk. If it is acceptable, the DAA issues the accreditation decision (i.e. Authorization to Operate (ATO), Interim Authorization to Operate (IATO), or Interim Authorization to Test (IATT)) and assigns an Authorization Termination Date on the DIACAP Scorecard. If the risk is unacceptable, a Denial of Authorization to Operate (DATO) will be issued.

E. Maintain Authorization to Operate and Conduct Reviews

In this activity, the DIACAP team works to maintain the Authorization to Operate (ATO) through the sustainment of an acceptable IA posture. This activity initiates and updates a Life cycle Implementation Plan for the IA controls that continuously monitors the system and assesses the quality of the IA controls.

F. Decommission

This activity reviews inheritance relationships to ensure the system's removal from operation does not negatively affect the operation of associated systems. The DIACAP registration information and system-related data are disposed of or updated to reflect the retiring of the system. The IS is then uninstalled or disconnected. A Denial of Authorization to operate is issued by the DAA and the system may no longer operate.

II. PROCESSES

A. Department Of State Continuous Certification And Accreditation Process

The Department of State has developed a process for continuous Certification and Accreditation (see Figure 2).

In second step is to Select Security Controls. The System Security Plan and system categorization are used to select Step one is Categorize Information System. The information system is categorized and the System Security Plan is created in this step.

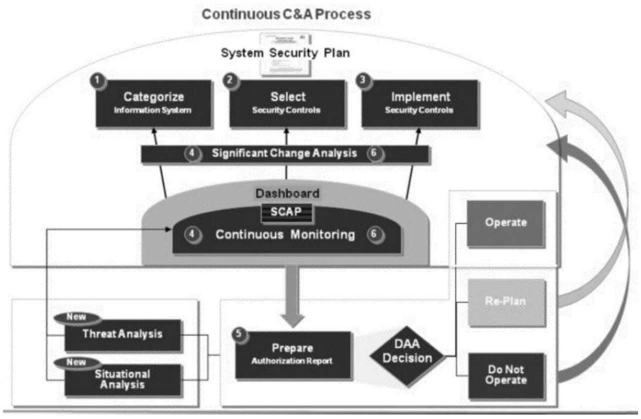


Fig. 2: Department of State Continuous C&A Process

The security controls. System specific controls are also selected as appropriate. The selected controls are implemented in the third step: Implement Security Controls. Significant Change Analysis is the fourth step in the process. The fifth step, Continuous Monitoring, combines the fourth and sixth steps of the RMF which involve testing at two stages of the process: during certification and during monitoring. The final step is to Prepare Authorization Report. With the opportunity to catch errors early due to continuous monitoring testing, reaching Do Not Operate status should be extremely rare [18].

B. Navy Transformational Certification And Accreditation Process

The Navy conducted a mapping between the DoDI 8500.2 and NIST SP 800–53 IA controls in order to combine the DIACAP and RMF processes into the Navy Transformational C&A Process. This process grew from the idea that "significant efficiencies can be gained through joint evaluations, and documentation, or overlapping security controls". This process consists of six events: Categorize Information System, Select Security Controls, Implement Security Controls, Assess Security Controls, Authorize Information System, and Monitor Security Controls. The tasks in each event are the combination of the DIACAP activities and RMF tasks.

C. Redundancy In The IA Processes

DISA has developed a mapping of the activities of the DIACAP to the steps in the RMF. The steps of the aforementioned processes have been represented in Table 1. The common structure is added as the last row of the table to highlight the extent of the redundancy between the processes. The concept proposed in this paper is to turn the common structure into a continuous monitoring process and reduce redundancy and time. This process can be implemented in a tool that can incorporate process-specific documents and tasks to combine the various IA processes and reuse common data such as assessment results. In this manner, conducting the continuous monitoring process will in effect perform all processes it encompasses. Further redundancy can be reduced by synchronizing inspection and certification dates so that the results of one are still valid and applicable to the others.

Process	Step 1	Step 2	Step 3	Step 4	Step 5	Step 6
DIACAP	Initiate and Plan IA C&A	Implement and Validate Assigned IA Controls	Make C&A Decision	Maintain ATO and Conduct Reviews	Decommission	
NIST RMF	Categorize Information System	Select Security Controls	Implement Security Controls	Assess Security Controls	Authorize Information System	Monitor Security Controls
DoS Continuous C&A Process	Categorize Information System	Select Security Controls	Implement Security Controls	Significant Change Analysis	Continuous Monitoring	Prepare Authorization Report
Navy C&A Transformational Process	Categorize Information System	Select Security Controls	Implement Security Controls	Assess Security Controls	Authorize Information System	Monitor Security Controls
Common Structure	Register or Update the System	Identify Security Controls	Implement Security Controls	Assess and Mitigate Security Controls	Determine and Accept Risk	Retire or Monitor the System

Table (1): Steps of Various IA Processes

D. Continuous Monitoring Process

Building upon the common structure discovered in Table 1, a continuous monitoring process has been developed. Figure 3 illustrates the process as a dynamic and flexible cycle with six activities

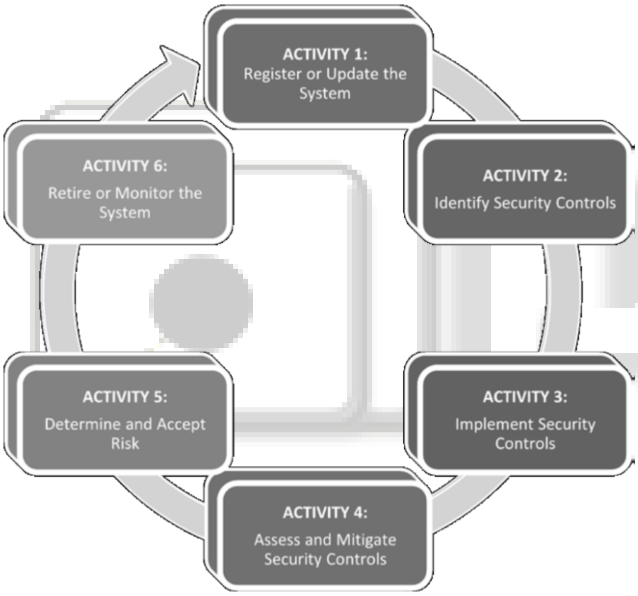

ACTIVITY 1:
Register or Update the System
ACTIVITY 2:
Identify Security Controls
ACTIVITY 3:
Implement Security Controls
ACTIVITY 4:
Assess and Mitigate Security Controls
ACTIVITY 5:
Determine and Accept Risk
ACTIVITY 6:
Retire or Monitor the System

Fig 3: Continuous Monitoring Process

The first activity in this cycle is to register or update the information system. If the information system (IS) is new, registration will describe the system, the responsible entity and organization, the location, and other information that will be used to generate the required documents. Second activity uses the categorization information from activity one to assign the applicable base controls to the IS, as described in DODI 8500.2. Each of these controls will be identified as applicable, inherited, or not applicable, and all applicable controls will be determined to be either implemented or not implemented. Third activity is the implementation of the relevant security controls in the Implementation Plan created in activity two. These controls are put into place and documented, as appropriate. All applicable controls should be implemented when activity four begins. In activity five, the risk to organizational operations (including mission, functions, image or reputation), organizational assets, individuals, other organizations, or the nation is determined and documented in the Risk Assessment. At the end of the system's life cycle, the system is decommissioned. The system registration information and system-related data are updated to reflect the system's removal from active status.

E. Other Ia Processes

Other IA processes include the Connection Approval Process (CAP) and Command Cyber Readiness Inspection (CCRI). The CJCSI 6211.02C, Defense Information System Network (DISN): Policy, Responsibilities and Processes, requires security controls to be in place in order for an IS to connect to the DISN and compliance inspections to be conducted to ensure the continuing effectiveness of these controls. The CAP ensures the IS is secure and has an ATO before allowing it to connect to the DISN. The CCRI provides a "quick look" assessment of the network security configuration of an IS and its compliance with DoD IA and computer network defense (CND) policies.

III. CONTINUOUS MONITORING CONCEPT

The Continuous Monitoring process is the underlying structure of most IA processes. If a tool is created with this underlying structure, it can be used to conduct the various IA processes and house the process artifacts. The proof-of-concept is designed as a three tiered web application that uses Java in order to connect the HTML pages with the PostgreSQL database. The database management system used is pgAdmin Version 1.12.3. The database is configured with constant tables, constant views, and user-specific tables. Constant tables are initialized in the development of the application but not changed by any user. The database contains constant views that are created in the development of the application but not changed by any user. The views show the controls for the nine possible combinations of MAC and CL. Duplicate controls are removed and if there are two levels for the same control, the more secure level is chosen. The views are:

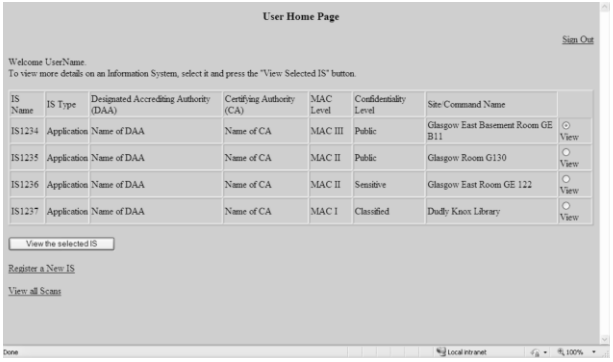
1) MAC_I_Public This view shows only the controls for a MAC I Public system.
2) MAC_I_Sensitive This view shows only the controls for a MAC I Sensitive system.
3) MAC_I_Classified This view shows only the controls for a MAC I Classified system.
4) MAC_II_Public This view shows only the controls for a MAC II Public system.
5) MAC_II_Sensitive This view shows only the controls for a MAC II Sensitive system.
6) MAC_II_Classified This view shows only the controls for a MAC II Classified system.
7) MAC_III_Public This view shows only the controls for a MAC III Public system.
8) MAC_III_Sensitive This view shows only the controls for a MAC III Sensitive system.
9) MAC_III_Classified This view shows only the controls for a MAC III Classified system.

A. Register Or Update The System

The environment the application uses is Apache Tomcat Version 6.0.28. It contains Catalina which is Tomcat's servlet container. The HTML pages are generated from the

Java classes in the apache folder when Catalina is initiated. The pages are then viewed via Internet Explorer Version 8 [9].

The pages are organized to implement the activities of the Continuous Monitoring Process.



User Home Page

Sign Out

Welcome UserName.
To view more details on an Information System, select it and press the "View Selected IS" button.

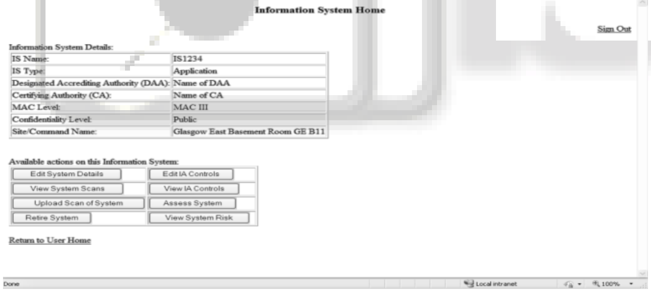
IS Name	IS Type	Designated Accrediting Authority (DAA)	Certifying Authority (CA)	MAC Level	Confidentiality Level	Site/Command Name	
IS1234	Application	Name of DAA	Name of CA	MAC III	Public	Glasgow East Basement Room GE B11	● View
IS1235	Application	Name of DAA	Name of CA	MAC II	Public	Glasgow Room G130	○ View
IS1236	Application	Name of DAA	Name of CA	MAC II	Sensitive	Glasgow East Room GE 122	○ View
IS1237	Application	Name of DAA	Name of CA	MAC I	Classified	Dudly Knox Library	○ View

Fig. 4: User Home Page

B. Information System Home

The ISHome page displays the details of the selected IS. From here the user can:

1) Edit or update the details of the IS (EditSystem page)
2) View the scans conducted on that particular IS (ISScans page)
3) Upload a scan of that IS (UploadScan page)
4) Retire the IS (RetireSystem page)
5) Edit the IA Controls for the IS (ISControls page)
6) View the IA Controls for the IS (ISControls page)
7) Assess the IS (AssessSystem page)
8) View/Accept the Risk of the IS (SystemRisk page)



Information System Home

Sign Out

Information System Details:

IS Name:	IS1234
IS Type:	Application
Designated Accrediting Authority (DAA):	Name of DAA
Certifying Authority (CA):	Name of CA
MAC Level:	MAC III
Confidentiality Level:	Public
Site/Command Name:	Glasgow East Basement Room GE B11

Available actions on this Information System:

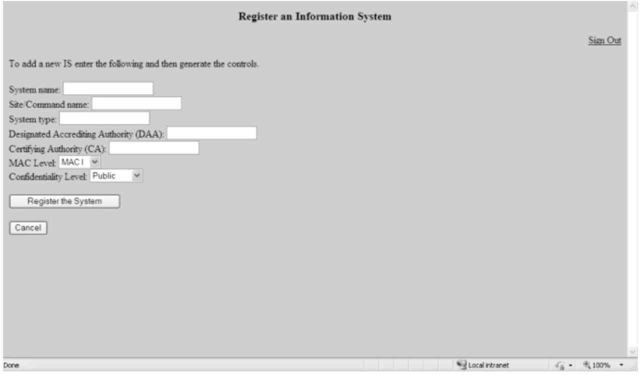
Fig 5: Information System Home Page

C. Register a System

The Register System page implements the Register part of Activity One of the Continuous Monitoring Process. It requests information from the user in order to register a new information system with the application. The information requested depends on the IA process or process step being carried out. See Figure 6 for a screenshot of the Register System page.

D. Edit a System

The Update part of Activity One of the Continuous Monitoring Process is implemented in the Edit System page. This page displays the same information that was requested in the Register System page but allows the user to edit the details. The user can save the changes and return to IS Home to view the updated details of the IS. If the user does not want the changes to be saved, the "Cancel" button will return them to the IS Home page without making any changes. not want the changes to be saved, the "Cancel" button will return them to the IS Home page without making any changes.



Register an Information System

Sign Out

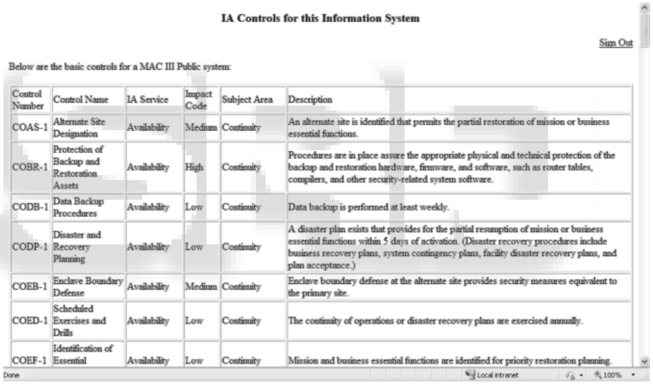
To add a new IS enter the following and then generate the controls.

System name:
Site/Command name:
System type:
Designated Accrediting Authority (DAA):
Certifying Authority (CA):
MAC Level: MAC I
Confidentiality Level: Public

Fig. 6: Register System Page

E. Identify Security Controls

Activity Two of the Continuous Monitoring Process is conducted in the IS Controls page. The application generates the base controls based on the MAC and CL of the IS. See Figure 7,8 for a screenshot of the IS Controls page. The user can then add or remove system-specific controls.



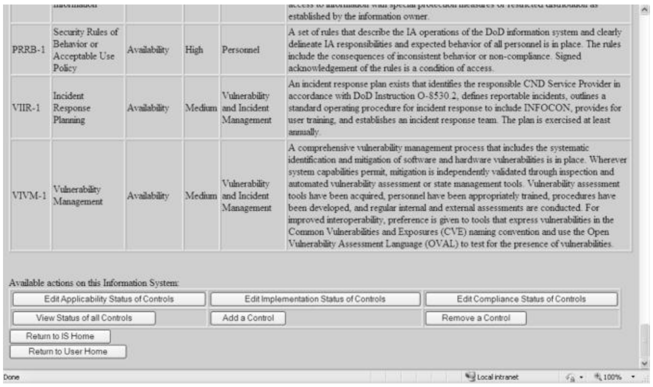
IA Controls for this Information System

Sign Out

Below are the basic controls for a MAC III Public system:

Control Number	Control Name	IA Service	Impact Code	Subject Area	Description
COAS-1	Alternate Site Designation	Availability	Medium	Continuity	An alternate site is identified that permits the partial restoration of mission or business essential functions.
COBR-1	Protection of Backup and Restoration Assets	Availability	High	Continuity	Procedures are in place assure the appropriate physical and technical protection of the backup and restoration hardware, firmware, and software, such as router tables, compilers, and other security-related system software.
CODB-1	Data Backup Procedures	Availability	Low	Continuity	Data backup is performed at least weekly.
CODP-1	Disaster and Recovery Planning	Availability	Low	Continuity	A disaster plan exists that provides for the partial resumption of mission or business essential functions within 5 days of activation. (Disaster recovery procedures include business recovery plans, system contingency plans, facility disaster recovery plans, and plan acceptance.)
COEB-1	Enclave Boundary Defense	Availability	Medium	Continuity	Enclave boundary defense at the alternate site provides security measures equivalent to the primary site.
COED-1	Scheduled Exercises and Drills	Availability	Low	Continuity	The continuity of operations or disaster recovery plans are exercised annually.
COEF-1	Identification of Essential	Availability	Low	Continuity	Mission and business essential functions are identified for priority restoration planning.

Fig 7:IS Control Pages



	information				access to information with special protection measures or restricted distribution as established by the information owner.
PRRB-1	Security Rules of Behavior or Acceptable Use Policy	Availability	High	Personnel	A set of rules that describe the IA operations of the DoD information system and clearly delineate IA responsibilities and expected behavior of all personnel is in place. The rules include the consequences of inconsistent behavior or non-compliance. Signed acknowledgement of the rules is a condition of access.
VIIR-1	Incident Response Planning	Availability	Medium	Vulnerability and Incident Management	An incident response plan exists that identifies the responsible CND Service Provider in accordance with DoD Instruction O-8530.2, defines reportable incidents, outlines a standard operating procedure for incident response to include INFOCON, provides for user training, and establishes an incident response team. The plan is exercised at least annually.
VIVM-1	Vulnerability Management	Availability	Medium	Vulnerability and Incident Management	A comprehensive vulnerability management process that includes the systematic identification and mitigation of software and hardware vulnerabilities is in place. Wherever system capabilities permit, mitigation is independently validated through inspection and automated vulnerability assessment or state management tools. Vulnerability assessment tools have been acquired, personnel have been appropriately trained, procedures have been developed, and regular internal and external assessments are conducted. For improved interoperability, preference is given to tools that express vulnerabilities in the Common Vulnerabilities and Exposures (CVE) naming convention and use the Open Vulnerability Assessment Language (OVAL) to test for the presence of vulnerabilities.

Available actions on this Information System:

Edit Applicability Status of Controls
Edit Implementation Status of Controls
Edit Compliance Status of Controls
View Status of all Controls
Add a Control
Remove a Control
Return to IS Home
Return to User Home
Done
Local intranet
100%

Fig. 8: IS Controls Page

F. Implement Security Controls

The user takes the Implementation Plan generated in the IS Controls page and implements the security controls. The Implementation Results are used to manually update the ImpStatus page, changing Not Implemented to Implemented on appropriate controls. Activity Three does not have its own page but makes use of the ImpStatus page.

G. *Assess And Mitigate Security Controls*

This includes Viewing the Scans page which displays all the scans conducted on the user's registered information systems, Upload Scan page requests information about the scan being uploaded and adds it to the table of scans; Assess the System page generates a Plan of Action and Milestone (POA&M) document from the results of the most recent scan of the IS, Mitigate Controls; there is no page for this in the proof-of-concept application because the user must do this outside of the application.

IV. RESULT

The proof-of-concept demonstrates the similar structure of the four IA processes as discussed. If the details of each process are removed, such as the tools used and documents generated, the construction of the process will look similar to this:

1) Register or Update the System
2) Identify Security Controls
3) Implement Security Controls
4) Assess and Mitigate Security Controls
5) Determine and Accept Risk
6) Retire or Monitor the System

The proof-of-concept takes the Continuous Monitoring Process presents it as an application. The application can be modified to turn the information on a particular IS into a process-specific document based on a template. In this manner, a larger tool can be developed that incorporates all relevant IA processes. Information can be shared and scans can be reused in order to avoid redundancy between submitting an IS through more than one process. If the processes are conducted around the same time, the information and scans will still be valid. This will reduce time as the user will not have to conduct another scan on the IS.52

REFERENCES

[1] Richard K. Betts, Conflict after the Cold War: Arguments on Causes of War and Peace, 3rd Edition. San Francisco: Pearson Education Inc., 2008, page 430.

[2] Committee on National Security Systems (CNSS), (2010, April 26). Instruction 4009, National Information Assurance Glossary. [Online]. Available: http://www.cnss.gov/Assets/pdf/cnssi_4009.pdf.

[3] United States Department of Justice, Office of Programs, (2002, December 17). Public Law 107–347, E-Government Act [includes Federal information Security Management Act (FISMA)]. [Online]. Available: http://it.ojp.gov/default.aspx?area=privacy&page=1287#contentTop.

[4] United States Department of Defense,(2002, October 24). Directive 8500.01E, Information Assurance (IA). [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.98

[7] Internet Explorer, "Internet Explorer – Web Browser for Microsoft Windows," Microsoft Corporation, September 2011, http://windows.microsoft.com/en-U.S./Internet-explorer/products/ie/home.

[8] United States Department of Defense,(2002, October 24). Directive 8500.01E, Information Assurance (IA). [Online]. Available: http://www.dtic.mil/whs/directives/corres/pdf/850001p.pdf.98

[9] Internet Explorer, "Internet Explorer – Web Browser for Microsoft Windows," Microsoft Corporation, September 2011, http://windows.microsoft.com/en-U.S./Internet-explorer/products/ie/home.