Federal Information Systems Continuous Monitoring Analysis

Posted on August 27, 2021

Introduction:

Information security continuous monitoring (ISCM) is a universal approach to risk management by providing controls with relevant high-level details and guidance on the modification of the system (Chenoweth, 2015). ISCM depicts a system with an organization-applicable risk framework with a well-defined control set. Risk management and its monitoring system can be potentially applied by enterprises with the proper assessment of the agency while allowing the combination of possible risk assessment and security. In this research paper, an overview of important concepts associated with ISCM will be highlighted along with an evaluation of the system.

Main Body:

Information security continuous monitoring (ISCM) has the ability to turn into the next big thing for the establishment of cyber security as well as risk management. Even though the federal agencies were able to find some challenges in the existing methodologies of ISCM, however, automated logging and current technology of ISCM help in handling the possible vulnerabilities in an effective way. NIST describes the major guidelines for an ISCM system developed for a federal organization. ISCM is effective as it manages to process the aggregated data.

Conclusion:

To conclude, the research paper will provide an overview of the ISCM system and its overall significance in federal agencies.

Introduction:

In the present-day environment, all organizations are dependent on technology and the services offered by it. The role of technology in mission-critical organizations is more significant. Moreover, the confidentiality and integrity of this technology turn into a critical mission as well. The development and design of an enterprise focus on different aspects; however, the design of security architecture is an important aspect as well. The organization now focuses on developing well-established IT infrastructures that help in meeting the governance structure, the missions carried out by them as

well as the business processes (Dempsey et al., 2011). Advancement of technology has opened avenues for possible security breach attacks, hence the dynamics of the information security process should be designed to manage the identification of the organization along with handling possible weakness that might become a threat to the organization's system. The architectural and operational environment of an organization is constantly changing, hence the information security system should address these changes as well (Ashenden, 2008).

Keeping in view the importance of information security and the need for its continuous change, a risk management framework (RMF) was developed by the National Institute of Standards and Technology (NIST, United States) to describe a system development lifecycle which combines information security and risk management activities (Vejvodová, 2019). RMF is significant because of the ongoing monitoring process (Khallaf & Majdalawieh, 2012). Within the limited resources of an organization, relevant and accurate information is required on time. Based on this aspect, a continuous monitoring system for information security was developed for mission critical-organizations. ISCM is defined as an ongoing maintenance and awareness system related to information security that handles threats and vulnerabilities to support the organization's risk management decisions (Dempsey et al., 2011). In this research paper, an overview of the background information on ISCM will be highlighted, along with the fundamental aspects of the system and its evolution of the system.

Background Information On ISCM:

Information security continuous monitoring (ISCM) is a universal approach to risk management by providing controls with relevant high-level details and guidance on the modification of the system (Vejvodová, 2019). ISCM depicts a system with an organization-applicable risk framework with a well-defined control set. Risk management and its monitoring system can be potentially applied by enterprises with the proper assessment of the agency while allowing the combination of possible risk assessment and security. Security is established on guidelines mentioned by NIST. The potential risk towards security can be reduced when modules are controlled, maintained, assessed and addressed properly by an organization. After the introduction of ISCM, a movement started about the use of ISCM at the federal level along with the United States Department of Defense based on the requirements of the US Federal Information Security Management Act (FISMA) (Dempsey et al., 2011).

Even though the compliance issues defined are mostly federal in nature, however, there are some important lessons in terms of technology improvement which can help different industries like finance and healthcare. In 2013, the United States Department of Homeland Security assisted federal agencies in buying monitoring software (Vejvodová, 2019). Along with the Homeland Security Department of the country, the U.S. Office of Management and Budget offered proper guidance on the working of continuous monitoring along with its ability to replace time-taking authorization cycles (Khallaf & Majdalawieh, 2012). Information security continuous monitoring (ISCM) has the ability to turn into the next big thing for the establishment of cyber security as well as risk management. Even though the federal agencies were able to find some challenges in the existing methodologies of ISCM,

however, automated logging and current technology of ISCM help in handling the possible vulnerabilities in an effective way.

NIST Institute in the United States researched the primary literature on Information security continuous monitoring (ISCM). NIST is responsible for the development of the information security standards along with the guidelines, which are the minimum requirements for the IT infrastructure of federal agencies (Clinton, 2015). Moreover, NIST provides a detailed guideline about the implementation of a risk management framework (RMF). Even though NIST has developed different publications on the ISCM in federal agencies, however, three key publications played an important part (Appendix A, Figure 1). ISCM has not been widely addressed and research for the well-being of federal agencies as the vast literature for ISCM is assessed in the fields of medical and sensor networks (Clinton, 2015). However, the current literature on ISCM for federal organizations and agencies provides an overview of the important concepts involved in ISCM for concerned federal-level agencies, along with the security references involved.

Important Concepts Involved In (ISCM) For Federal Information Systems And Organizations:

ISCM for federal information systems and organizations have strategies that are developed and evolved on the basis of a risk-based decision-making system and on the requirements of information management (Clinton, 2015). In the case of federal agencies, these requirements are defined as a standard by NIST and specified by the federal agency ISCM will operate. For instance, security breach management in ISCM for NASA will differ in comparison to the system developed for the intelligence department. Most federal organizations implement the ISCM system based on the requirements defined by individuals accountable and responsible for managing organization security along with the possible risk tolerance. Every organization has a different set of resources, such as available tools/applications and policies. Hence, the implementation of ISCM is done on the basis of minimum utilization of organizational resources with a standard defined (Clinton, 2015). Moreover, ISCM implementation in federal agencies is done to give maximum leverage to the information security system. Once the analysis is done by ISCM, the possible organizational risk is mentioned after the discrete set of processes are performed (Dempsey et al., 2011).

One of the major benefits gained by federal agencies with the implementation of the ISCM is the situation analysis provided by the system (Khallaf & Majdalawieh, 2012). ISCM provides awareness about the security system of the federal information system based on the situation faced along with the information collected from different resources. Information-collecting resources generally include technology, processes, and people. With the situation awareness provided, ISCM holds the tendency to react to the situation change encountered. In most of the federal agencies fighting for the establishment of an organization-wide risk management system, ISCM is defined as a well-developed tactic for information security protection and risk assessment. For instance, many organizations use

security-related information that potentially affects the component inventory of the system as a way of aligning with the information system component inventory.

With the monitoring capabilities offered by ISCM, federal agencies use the situation awareness offered by the system to increase and improve the agency's overall security. Moreover, better insights related to security process control help in increasing situational awareness among the employees working in the IT infrastructure of the organization. Hence, the implementation of ISCM is defined as a recursive process.

An Overview Of The Working Of ISCM In Federal Agencies:

Since ISCM is a recursive process, hence input and output of security-related information are dependent on the communication between ISCM and the agency's security processes (Madsen, 2013). The involvement of associated requirements in this communication is essential for input and output. From this, it can be assessed that the collection of data is an important part of calculating the metrics for the security control process. However, research suggests that once the issue is identified in the security system of an agency, the diagnosed problem holds the tendency to trigger one or more controls across the information system of the agency, such as updating the relevant security information and modification of the security program of the organization. Hence, an improved version of organization-wide risk management will be received at the end of data communication, assessment, and the security handling procedure of ISCM. Continuous improvement of the ISCM system depends on the collection of information and the corresponding findings (Madsen, 2013). Once the information is collected, it is assessed if the information is effective or not. For instance, in a security system, managing the important inventory of the system's effective information will highlight whether the inventory is accurate or not.

In any case, if the findings are termed ain s inaccurate, then the system looks for possible root causes which led to the inaccuracy found in the results. Some of the root causes may include that the agency's system has been attacked or network components are not connected in order. Based on the root problem identified, the relevant response is initiated by the system. For example, in the example of the weapon inventory system, the responsible parties will be notified about the inventory update (Madsen, 2013). Moreover, security-related information helps in coming up with pre-defined metrics for the system. Accurate system components' vulnerabilities improve the security domains of the system and offer better management of possible vulnerabilities in the system.

Evaluation Of ISCM With Risk Management

Framework:

One of the six steps of the Risk Management Framework is continuous monitoring (Dempsey et al., 2011). While choosing a framework, the most critical step is the selection of a framework that provides support to the operations and also controls that assist the organization in compliance purposes. The determination can be seen across four zones of security, administration, task performance and administration. Since the aim is to ensure that all the tasks are performed effectively, therefore, Information Assurance (IA) is a significant part of all these aspects (Dempsey et al., 2011). All these zones play a significant role in carrying out this mission effectively. In order to ensure the effectiveness of the work, there have been quite a few updates in order to address the issue of risk management. Among these updates, but the most protruding among these updates is NIST SP 800-37 combined with the NIST SP 800-53 and NIST SP 800-137 (Clinton, 2015). With the assistance of these documents, the information Assurance of risk management can be addressed effectively in a continuous manner.

The guidance for applying the risk management program to an organization is carried with the assistance of NIST SP 800-37 (Clinton, 2015). As the sorts of complex, efficient assaults have expanded, the potential for more elevated levels of harm to national security has expanded as well. For federal organizations to comprehend their odds of turning out to be undermined and the harm is done from that bargain, an arrangement of nonstop appraisal of vulnerabilities, effects, alleviations, and lingering hazard acknowledgment ought to be received. Without an extensive framework set up, an association is basically leaving itself open to risk. SP 800-37 accommodates that framework and methods for executing it, however, it is dependent upon the association to tailor and contrivance this in an effective manner (Clinton, 2015). The procedure includes the following steps:

- Categorize data frameworks
- Select security control
- Execute security controls
- Evaluate security controls
- Approve data frameworks
- Monitoring security controls

SP 800-37 helps in assessing the level of risk faced by any organization (Dempsey et al., 2011). The degree of consistency with setup security controls can give the administration possible thoughts about the general hazard level of the association, just as give direction on what territories ought to be improved through strategy, innovation or workforce.

Reference For Security Controls:

The controls that are a part of a framework are a significant part of risk management. With the assistance of control compliance, SP 800-53 uses a multi-tiered method (Dempsey et al., 2011). This

method includes an effective security control, security control standards, and security control frameworks. The overlaid controls of a risk management framework in an organization operation along with SP 800-53 and SP 800-37 (Khallaf & Majdalawieh, 2012). The selection of these controls is highly based on the information stored by the system. These controls are applied is a proposed order where higher priorities are held first in the controls. These controls include documentation and verification, incident scheduling, confrontation responses, preservation, probability valuation and the protection of the media (Vejvodová, 2019).

Pros And Cons Of Using Information Security Continuous Monitoring (ISCM):

One of the major advantages of using the ISCM model is that the system is able to capture aggregate data from already existing systems. With the help of this automated process, information is updated in a timely manner along with a review by the leadership (Chenoweth, 2015). However, a loophole is present in the ISCM system as not all the activities work in an automated manner. Logging and capturing automatically may not be easy in Information security continuous monitoring (ISCM). Moreover, no guidelines are highlighted by NIST for managing manual logging. In NIST SP 800-137, manual checks need to be compatible with the automated checks (Reddick, 2017). Overall, ISCM covers maximum risk assessment and monitoring based on NIST guidelines.

Conclusion:

To conclude, Information security continuous monitoring (ISCM) provides a system that monitors and assesses the possible threats and vulnerabilities of an organizational system. Based on the guidelines proposed by NIST, federal agencies are now implementing ISCM as a part of their work so that the systems are updated on time in case a possible threat is identified (Chenoweth, 2015). ISCM works on the basis of the findings and information gathered. Data aggregation is one of the major benefits of ISCM. Overall, ISCM has proved effective for the working of federal agencies.

References

Ashenden, D. (2008). Information Security management: A human challenge?. *Information Security Technical Report*, *13*(4), 195-201. https://doi.org/10.1016/j.istr.2008.10.006

Clinton, L. (2015). Federal Cyber security Best Practices. *Journal Of Strategic Security*, *8*(4), 53-68. https://doi.org/10.5038/1944-0472.8.4.1456

Dempsey, K., Chawla, N., Johnson, L., Johnston, R., Jones, A., & Orebaugh, A. et al. (2011). Information Security Continuous Monitoring (ISCM) for federal information systems and organizations.

https://doi.org/10.6028/nist.sp.800-137

Khallaf, A., & Majdalawieh, M. (2012). Investigating the Impact of CIO Competencies on IT Security Performance of the U.S. Federal Government Agencies. *Information Systems Management*, *29*(1), 55-78. https://doi.org/10.1080/10580530.2012.634298

Vejvodová, P. (2019). Information and Psychological Operations as a Challenge to Security and Defence. *Vojenské Rozhledy*, *28*(4), 83-96. https://doi.org/10.3849/2336-2995.28.2019.03.083-096

Madsen, W. (2013). Reinventing Federal Security Policy: A Failed Effort. *Information Systems Security*, *4*(1), 11-15. https://doi.org/10.1080/10658989509342484

Reddick, C. (2017). Collaboration and Homeland Security Preparedness: A Survey of U.S. City Managers. *Journal Of Homeland Security And Emergency Management*, *5*(1). https://doi.org/10.2202/1547-7355.1414

National Institute of Standards and Technology Information Technology Guide. (2004), *26*(6), 48. https://doi.org/10.1097/01445442-200411000-00014

Chenoweth, J. (2015). Information Security Policies, Procedures, and Standards: Guidelines for Effective Information Security Management. *Journal Of Information Privacy And Security*, *1*(1), 43-44. https://doi.org/10.1080/15536548.2005.10855762

Appendix A

Figure 1: Key NIST special publications related to ISCM (Clinton, 2015)