ISCM Plan

Daniel Carbajal

CIS608

11.2-Written Assignment

February 23, 2022

This paper presents the process of developing information security continuous monitoring (ISCM) which is defined as maintaining ongoing awareness of information security, vulnerabilities, and threats to support organizational risk management decisions. One must maintain situational awareness across all the systems in the organization. This can be done by monitoring, maintaining, and constantly updating its security protocols to implement new changes to the security systems and controls as the systems change or become vulnerable to an attack. Different security systems will be monitored to include physical security such as alarms and CCTV cameras, company devices such as routers, servers, desktops, and mobile devices, and software and applications uses within the company. A security guard or a third-party company can be hired to provide 24/7 monitoring of the physical security and another third-party systems company that can work with IT personnel to monitor against threats on equipment and software systems. Training will be provided to ensure that all employees know about the company’s security practices and can also monitor and report any incidents they may come across. Overall, monitoring will be done consciously by all parties including all the tiers of the organization.

All the following security controls will be used:

* AC-18(3) WIRELESS ACCESS | DISABLE WIRELESS NETWORKING
* AT-2(1) LITERACY TRAINING AND AWARENESS | PRACTICAL EXERCISES
* AU-12(1) AUDIT RECORD GENERATION | SYSTEM-WIDE AND TIME-CORRELATED AUDIT TRAIL
* CA-6(1) AUTHORIZATION | JOINT AUTHORIZATION — INTRA-ORGANIZATION
* CM-7(1) LEAST FUNCTIONALITY | PERIODIC REVIEW
* CP-2(1) CONTINGENCY PLAN | COORDINATE WITH RELATED PLANS
* IA-5(1) AUTHENTICATOR MANAGEMENT | PASSWORD-BASED AUTHENTICATION
* IR-4(1) INCIDENT HANDLING | AUTOMATED INCIDENT HANDLING PROCESSES
* MA-4(1) NONLOCAL MAINTENANCE | LOGGING AND REVIEW
* E-2(1) PHYSICAL ACCESS AUTHORIZATIONS | ACCESS BY POSITION OR ROLE
* PL-7 SYSTEM SECURITY AND PRIVACY PLANS
* PS-5 PERSONNEL TRANSFER
* RA-3(1) RISK ASSESSMENT | SUPPLY CHAIN RISK ASSESSMENT
* SA-5 SYSTEM DOCUMENTATION
* SC-12(1 CRYPTOGRAPHIC KEY ESTABLISHMENT AND MANAGEMENT | AVAILABILITY
* SI-4 SYSTEM MONITORING
* SR-10 SYSTEM MONITORING

These controls will provide the framework for developing the ISCM to include the implementation of the security systems down to the documentation and constant monitoring of all security and equipment used by the company. Communications of security status will be cone across all tiers of the organization, from information processes, business processes, and the organization. This will be done by incorporating the two automated controls

* Event Management
* Configuration Management

Event management involves monitoring and responding to observable occurrences in a network or system. Various tools and technologies exist to monitor events, such as intrusion detection systems and logging mechanisms The implementation and effective use of logging and log management tools and technologies can assist organizations in automating the implementation, assessment, and continuous monitoring of several NIST SP 800-53. Configuration management tools allow administrators to configure settings, monitor changes to settings, collect setting status, and restore settings as needed. Managing the numerous configurations found within information systems and network components has become almost impossible using manual methods thus automation systems will be used.

To enhance the ability to identify inappropriate or unusual activity, organizations may integrate the analysis of vulnerability scanning information, performance data, network monitoring, and system audit record (log) information through the use of SIEM tools. SIEM tools are a type of centralized logging software that can facilitate the record and aggregation of data. A SIEM tool will be used to Audit Review, Analyze, and Report on the systems that are being constantly monitored and are automated to perform certain tasks such as an attack or a configuration management action to report and mitigate the actions.

**References**

ISCM, <https://csrc.nist.gov/publications/detail/sp/800-137/final>

Mattord, H., & Whitman, M. (2016). Management of Information Security (5th ed.). CENGAGE Learning Custom Publishing.