Information Security Continuous Monitoring (ISCM) Plan

Keith M. Hall

College of Science and Technology, Bellevue University

CIS608-T301: Information Security Management

Professor Kayleen Amerson

November 13, 2022

Information Security Continuous Monitoring (ISCM) Plan

Organizations need to keep an eye on their information security measures. Automated solutions that monitor installed technological measures in real time can give an organization a far more dynamic perspective of the efficiency of those controls and the organization's security posture. An ISCM program is set up to gather data using information already available in line with pre-established metrics. The NIST Special Publication (SP) 800-137 offers instructions for creating an Information Security Continuous Monitoring (ISCM) program that may be used at all organizational levels as a risk management and decision-support tool. Additionally, continuous monitoring is an essential component of the risk management process that guarantees that activities across the entire business continue to be at an acceptable level of risk despite any changes that take place. Furthermore, when resources are scarce and organizations must prioritize their efforts, timely, pertinent, and reliable information is even more important. (NIST Laboratory Information Systems Team, Problem Processing Request, n.d.-e). This paper presents the Information Security Continuous Monitoring (ISCM) plan for CP Dental to explain how the organization plans to maintain situational awareness, assess all security controls, and provide actionable communication of security status across all tiers of the organization.

INTRODUCTION

Scope

This Information System Continuous Monitoring (ISCM) Plan applies to all employees of CP Dental. As directed, key personnel will be appointed to perform duties in support of the ISCM. All devices and data within the system boundary, as documented in the system authorization, fall under the requirements of this plan.

Roles and Responsibilities

The following individual is responsible for developing, implementing, coordinating, complying with, and maintaining the Continuous Monitoring Plan and its associated mechanisms:

- **The agency head** will serve as the Chief Information Officer within the context of the sole risk executive who leads the organization's ISCM program. The agency head will ensure that an effective ISCM program is established and implemented for the organization by establishing expectations and requirements for the organization's ISCM program.

CONTINUOUS MONITORING REQUIREMENTS

Continuous monitoring will allow CP Dental to maintain situational awareness of all systems across the organization and an understanding of threats and threat activities every month.

Metrics

- Change in the number and severity of vulnerabilities revealed and remediated.
- Change in the number of unauthorized admin account access attempts.
- Monitor subnets/Internet protocol (IP) addresses.
- Network traffic monitoring.

Network Monitoring Tools

- Aggregation of similar log entries will be kept into a single count of the number of security occurrences that occur monthly.
- CP Dental will use SourceForge.net for open-source monitoring software, CERT organizations, and public network sources like the National Vulnerability Database.
- SolarWinds NetFlow Traffic Analyzer for automated monitoring

SECURITY ASSESSMENTS AND AUTHORIZATIONS

- Whether manual or automated, the data collected will be assembled for analysis and reported to the organizational source charged with correlating and analyzing it in ways that are relevant for risk management activities.
- The information to be analyzed will be provided to organizational sources as recurring reports, automated reports, and data feeds.

CP Dental will use standardized methodologies to facilitate efficiencies, intra-tier information exchange, correlation, and other analysis for actionable communication of security status across all tiers of the organization.

Reference List

NIST Laboratory Information Systems Team - Problem processing request. (n.d.-e). https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-137.pdf

(NIST Laboratory Information Systems Team - Problem Processing Request, n.d.-e)

Whitman, M. E., & Mattord, H. J. (2018). Management of Information Security (6th ed.). Cengage Learning.

https://www.isaca.org/resources/isaca-journal/issues/2015/volume-1/information-security-continuous-monitoring-the-promise-and-the-challenge

What's ISCM? (NIST SP 800-137). (2020, September 2). IT perfection - Network Security. https://www.itperfection.com/network-administration/whats-iscm-nist-sp-800-137-network-security-cybersecurity-bcp-disaster-recovery-information/