Security Assessment Report (SAR)

CYB 610: Cyberspace and Cybersecurity Foundations

Professor Name

University of Maryland University College

Abstract

The purpose of the security assessment plan (SAR) is to communicate the results of security assessments of the information technology (IT) infrastructure to include its: people, processes, policies and information systems (NIST, 2010). The SAR is one of the main documents included in the system authorization package, along with the system security plan (SSP) and plan of actions and milestones (POA&Ms). These documents are used to provide the authorizing official (AO) with necessary feedback on the security state and posture of the system to make a risk-based decision if the system should operate or continue operations. The SAR provides the overall state of security of the IT infrastructure detailing the infrastructure's ability to meet the security objectives: Confidentiality, Integrity, and Availability (CIA) when protecting the data that is transmitted, stored, or processed by and through it. Although the SAR is s document that captures a snapshot in time of the security state of the information system; to support continuous monitoring activities, the SAR is updated whenever subsequent security assessments are performed. To support document revision, the SAR should be annotated with updated versions each time it is changed and these changes should be annotated within the SAR itself. According to NIST (2014), the key elements to an assessment report is outlined in Appendix G (pp G-2); however, for this SAR the following elements will be included: Operating System (OS) Overview, OS Vulnerabilities, Assessment Methodologies, Risk, and Recommendations.

OS Overview

Operating System (OS)

User's Role in OS.

Kernel and OS Applications.

OS Types.

OS Vulnerabilities

Windows Vulnerabilities

Intrusion Methods.

Linux Vulnerabilities

Intrusion Methods.

MAC Vulnerabilities

Mobile Device Vulnerabilities

Risk

Accepting Risk

Transferring Risk

Mitigating Risk

Eliminating Risk

Security Tools

Intrusion Detection System (IDS)

Intrusion Prevention System (IPS)

Vulnerability Assessment Methodology

Microsoft Baseline Security Analyzer (MBSA)

OpenVAS

Assessment Tool Comparative Analysis

Similarities.

Differences.

Recommendations

Conclusion

References

National Institute of Standards and Technology (NIST) (2014). Assessing security and privacy controls in federal information systems and organizations. *NIST Special Publication 800-53A Revision 4.* Retrieved from http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53Ar4.pdf

National Institute of Standards and Technology (NIST) (2010). Guide for applying the risk management framework to federal information systems. *NIST Special Publication 800-37 Revision 1.* Retrieved from http://csrc.nist.gov/publications/nistpubs/800-37-rev1/sp800-37-rev1-final.pdf

.