Creating the SAR 8-10 page double-spaced APA and RAR 5-6 page double-spaced APA.

Your research and exercises have led you to this moment: creating your SAR and RAR . Consider what you have learned in the previous steps as you create your reports for leadership.

Prepare a Security Assessment Report (SAR) with the following sections:

1.Purpose

2.Organization

3.Scope

4.Methodology

5.Data

6.Results (I will input)

7.Findings (I will input)

The final SAR does not have to stay within this framework, and can be designed to fulfill the goal of the security assessment.

Prepare a Risk Assessment Report (RAR) with information on the threats, vulnerabilities, likelihood of exploitation of security weaknesses, impact assessments for exploitation of security weaknesses, remediation, and cost/benefit analyses of remediation. Devise a high-level plan of action with interim milestones (POAM), in a system methodology, to remedy your findings. Include this high-level plan in the RAR. Summarize the results you obtained from the vulnerability assessment tools (i.e., MBSA and OpenVas) in your report.

Step 1: Organizational Background

Perform quick independent research on organizational structure in your industry sector. Describe the background of your organization, including the purpose, organizational structure, the network system

description, and a diagram of the organization. Include LAN, WAN, and systems in diagram format (use the OPM systems model of LAN side networks), the intra-network, and WAN side networks, the inter-net. Identify the boundaries that separate the inner networks from the outside networks.

This information can be fictitious, or modeled from existing organizations. Be sure to cite references.

Step 2: Organizational Threats

You just provided detailed background information on your organization. Next, you'll describe threats to your organization's system. Before you get started, select and explore the contents of the following link: insider threats (also known as internal threats). As you're reading, take note of which insider threats are a risk to your organization.

Now, differentiate between the external threats to the system and the insider threats. Identify where these threats can occur in the previously created diagrams. Define threat intelligence, and explain what kind of threat intelligence is known about the OPM breach. Relate the OPM threat intelligence to your organization. How likely is it that a similar attack will occur at your organization?

Review the information captured in these two links message and protocols and Transmission Control Protocol/Internet Protocol (TCP/IP), and identify any security communication, message and protocols, or security data transport methods used such as (TCP/IP), SSL, and others. Make note of this, as it should be mentioned in your reports.

You have a suite of security tools, techniques, and procedures that can be used to assess the security posture of your organization's network in a SAR.

Next, examine these resources on firewalls and auditing–RDBMS related to the use of the Relational Database Management System (i.e., the database system and data) RDBMS. Also review these resources related to access control.

Determine the role of firewalls and encryption, and auditing – RDBMS that could assist in protecting information and monitoring the confidentiality, integrity, and availability of the information in the information systems.

Reflect any weaknesses found in the network and information system diagrams previously created, as well as in the developing SAR.

You know of the weaknesses in your organization's network and information system. Now you will determine various known threats to the organization's network architecture and IT assets.

Get acquainted with the following types of threats and attack techniques. Which are a risk to your organization?

•IP address spoofing/cache poisoning attacks

•denial of service attacks (DoS)

•packet analysis/sniffing

•session hijacking attacks

•distributed denial of service attacks

In identifying the different threats, complete the following tasks:

1.Identify the potential hacking actors of these threat attacks on vulnerabilities in networks and information systems and the types of remediation and mitigation techniques available in your industry, and for your organization.

2.Identify the purpose and function of firewalls for organization network systems, and how they address the threats and vulnerabilities you have identified.

3.Also discuss the value of using access control, database transaction and firewall log files.

4.Identify the purpose and function of encryption, as it relates to files and databases and other information assets on the organization's networks.

Include these in the SAR.

Note: Hackers frequently scan the Internet for computers or networks to exploit. An effective firewall can prevent hackers from detecting the existence of networks. Hackers continue to scan ports, but if the hacker finds there is no response from the port and no connection, the hacker will move on. The firewall can block unwanted traffic and NMap can be used to self-scan to test the responsiveness of the organization's network to would-be hackers

Risk and Remediation

What is the risk and what is the remediation? What is the security exploitation? You can use the OPM OIG Final Audit Report findings and recommendations as a possible source for methods to remediate vulnerabilities.

Read this risk assessment resource to get familiar with the process, then prepare the risk assessment. Be sure to first list the threats, then the vulnerabilities, and then pairwise comparisons for each threat and vulnerability, and determine the likelihood of that event occurring, and the level of impact it would have on the organization. Use the OPM OIG Final Audit Report findings as a possible source for potential mitigations. Include this in the risk assessment report (RAR).