**Student Number: A00329339**
**Student Name: Temitayo Fisher**

## Gap Analysis Plan and Risk Assessment Methodology

**Scenario:**
After the productive team meeting, Fullsoft's chief technology officer (CTO) wants further analysis performed and a high-level plan created to mitigate future risks, threats, and vulnerabilities. As part of this request, you and your team members will create a plan for performing a gap analysis and then research and select an appropriate risk assessment methodology to be used for future reviews of the Fullsoft IT environment.

An IT gap analysis may be a formal investigation or an informal survey of an organization's overall IT security. The first step of a gap analysis is to compose clear objectives and goals concerning an organization's IT security. For each objective or goal, the person performing the analysis must gather information about the environment, determine the present status, and identify what must be changed to achieve goals. The analysis most often reveals gaps in security between "where you are" and "where you want to be."

Two popular risk assessment methodologies are NIST SP 800-30 revision 1, Guide for Conducting Risk Assessments, and Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE). Your focus will be on the OCTAVE Allegro version, which is a more concise version of OCTAVE. When reviewing the methodologies, consider the following:

- Which features or factors of each methodology are most important and relevant to Fullsoft?

  **NIST SP 800-30 rev. 1:**
  - The risk management framework delivers complete instructions to identify and evaluate and rank various risks.
  - Organizations need to focus on creating risk assessment followed by mitigation strategies for successful management according to this framework.
  - Detailed risk assessment process: Offers a step-by-step risk assessment process.

  **OCTAVE Allegro:**
  - Operational and business impact focus: Focuses on the operational and business impacts of risk.
  - Risk evaluation processes with this model undergo simplicity and efficiency within their risk assessment methods.
  - Critical asset and threat identification functions as a core emphasis point because organizations must discover their vital assets as well as their threats.

- Which methodology is easier to follow?

  OCTAVE Allegro provides the most straightforward process for adhering to procedures according to the presented scenario. OCTAVE Allegro stands as an ideal risk assessment method for small businesses such as Fullsoft because it delivers a simplified and condensed risk assessment solution.

- Which methodology appears to require fewer resources, such as time and staff, but still provides for a thorough assessment?

  OCTAVE Allegro needs less staffing and time commitment to deliver a complete risk evaluation according to the scenario. Fullsoft benefits from OCTAVE Allegro because its risk assessment protocol streamlines the procedure to fit their organizational limitations.

**Tasks**
Create a high-level plan to perform a gap analysis.
Review the following two risk assessment methodologies:

- NIST SP 800-30 rev. 1, Guide for Conducting Risk Assessments (formerly titled " Risk
- Management Guide for Information Technology Systems")
- Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Allegro version
- Create a report that includes the gap analysis plan, a brief description of each risk assessment methodology, a recommendation for which methodology Fullsoft should follow, and justification for your choice.

**Introduction:**

Modern organizations need to develop an ongoing procedure for security posture assessment and enhancement in our present evolving cybersecurity environment. Fullsoft develops risk assessment methodology alongside structured gap analysis efforts to minimize potential threats and vulnerabilities and risks. The document describes a plan to conduct gap analysis while evaluating the risks assessment schemas which include NIST SP 800-30 Revision 1 and OCTAVE Allegro. The suggestion follows Fullsoft’s requirements.

**High-Level Gap Analysis Plan:**

The current IT security status at Fullsoft undergoes evaluation to determine gaps versus their intended security targets. This plan describes the complete operation which includes the following stages:

**Step 1:** Define Security Objectives

- The first step involves determining both business objectives along with security requirements.
- Security improvement requires the definition of fundamental performance indicators labeled key performance indicators.

**Step 2:** Assess Current Security Posture

- IT security personnel along with teams responsible for security will undergo interview and survey evaluation.
- Security operations should examine all present security guidelines along with crisis management protocols while verifying that organizations satisfy all legal standards.
- The organization should perform vulnerability assessments and security audits.

**Step 3:** Identify Gaps

- Compare current security posture against industry standards (e.g., NIST Cybersecurity Framework, ISO 27001).
- Team members must identify system weaknesses along with unhandled threats and non-compliance violations.
- Risk assessment will proceed through Step 4 before establishing action plans.
- Sort gaps for assessment according to their risk levels which include low, medium and high.
- Executive management should approve suggested remediation solutions which combine policy adjustments with implementation of technical barriers and staff education programs.

**Step 5:** Implement and Monitor Improvements

- The organization must execute remediation strategies according to their established priority.
- Security controls should be monitored for constant assessment and the analysis needs periodic updates.

**Review of Risk Assessment Methodologies:**

**NIST SP 800-30 Revision 1**

The NIST Special Publication 800-30 Revision 1 serves as an extensive reference for carrying out risk assessment activities. The approach follows specific methods that organize assessment work in these stages:

- **Risk Framing:** Risk Framing serves as the foundation to determine how organizations should perform their risk assessments.
- **Risk Assessment:** Risk Assessment functions as a process to identify weaknesses while performing a thorough analysis and deciding on the corresponding risk levels.
- **Risk Response:** The response stage creates appropriate mitigation approaches using the assessment findings.
- **Risk Monitoring:** Risk monitoring consists of analyzing controls together with ongoing observation of identified risks.

The government and enterprise sector implements NIST SP 800-30 risk management standards because they need detailed and standardized risk management approaches.

**OCTAVE Allegro**

The streamlines edition of OCTAVE called OCTAVE Allegro enables users to assess information assets alongside their security dangers.

Key Components of OCTAVE Allegro:

- **Establish Risk Criteria:** Risk tolerances and impact levels need to be defined as primary risk criteria.

- **Identify Information Assets:** Organizations should identify their information assets by listing down critical elements including customer data, intellectual property and IT infrastructure.
- **Analyze Threats and Vulnerabilities:** The evaluation process analyzes both existing system vulnerabilities and potential threats starting from internal staff members up to external cyberattacks.
- **Assess Security Risks:** Risks need to be evaluated according to their estimated consequences and chance of occurrence.
- **Develop Risk Mitigation Strategies:** Security controls together with risk mitigation action plans need to be devised for addressing the highest priority risks.

**Recommendation and Justification:**

Fullsoft needs OCTAVE Allegro as its preferred risk assessment methodology to fulfill business requirements. The adoption of OCTAVE Allegro as preferred risk assessment methodology stands justified by the following points:

- The key strength of OCTAVE Allegro over NIST SP 800-30 lies in its explicit concentration on safeguarding essential information resources which adhere to Fullsoft's organizational structure.
- Refined and Compact Implementation – OCTAVE Allegro presents an organized method with short procedures that suits the mid-sized Fullsoft organization well.
- The methodology delivers explicit instructions about effective methods to handle risks.
- Organizations which need a customizable framework to handle changing security needs can find OCTAVE Allegro suitable for their assessment requirements.

**Implementation Strategy for Fullsoft:**

- **Training & Awareness:** The organization should provide training sessions to educate employees about OCTAVE Allegro methods alongside general cybersecurity best practices.
- **Execution:** The risk assessment methodology requires execution through its designated procedures.
- **Integration:** Align findings with ongoing gap analysis efforts.
- **Continuous Monitoring:** The institution should monitor all processes on a constant basis to revise and maintain their risk mitigation programs and updates.

The combination of a structured gap analysis with OCTAVE Allegro risk assessment capabilities at Fullsoft will strengthen its cybersecurity framework. Through this plan the organization can track down security risks properly then sort them for successful protection of the security condition.

**References:**


- *NIST Special Publication 800-30 Revision 1: Guide for Conducting Risk Assessments.*
- *OCTAVE Allegro: Carnegie Mellon University, Software Engineering Institute.*
- *ISO/IEC 27001: Information Security Management Standard.*
- *NIST Cybersecurity Framework: National Institute of Standards and Technology.*