Fullsoft Gap Analysis Redo

Fernando D. Parra

Metropolitan State University of Denver

CSS-2754-001 Host Security

Maranda Mulder

February 29th, 2024

Fullsoft Gap Analysis Redo

The comparison between the current shape of Information Technology risk and the expected shape is a substantial method to set adequate security controls and frameworks that must be put in place for Fullsoft to strengthen its overall security posture. Identifying the gaps will enable Fullsoft to prioritize its efforts and resources effectively, ensuring critical vulnerabilities are managed appropriately.

High-Level Plan

To perform the requested gap analysis plan, it is essential to set two key phases, a desired state of what Fullsoft is trying to achieve and the current state of what Fullsoft has already enforced. By comparing these two phases, Fullsoft can identify disparities representing areas in need of improvement. A detailed comprehension of the gap between aspiration and reality will prepare the growth of actionable recommendations for Fullsoft's security posture.

Choose the Proper Framework

For instance, let's begin with a baseline to set the guidelines; Fullsoft may use a specific standard(s) to perform its goal, the NIST SP 800-37, 53, 171, NIST CSF, or ISO/IEC 27001. Fullsoft is a large company developing software, thus it is only suitable to use an official and detailed framework like NIST SP 800-30 which is intended for large organizations, corporations, and companies. The NIST Guide for Risk Assessment is excellent and includes NIST SP 800-37 or Risk Management Framework that complements the objectives of Fullsoft's CSO.

Objectives and Goals

The objectives and goals that Fullsoft's Chief Security Officer expectations are mitigating risks, threats, as well as vulnerabilities thus let the analysis start there to illustrate what security is going to be needed in the future. Although the process of performing a gap

analysis with a high-level project plan can be a task of up to years, depending on the size of the organization (in Fullsoft's case, a large company), it is vital to develop a collection of steps in a concise and clear pattern to select parts of the security policy and industry standards that can be applied.

Current State

The baseline should also include an examination of crucial assets, gathering detailed information for both logical and physical components, an evaluation of the employees, and the current processes, standards, and procedures being executed at Fullsoft, this part of the gap analysis includes reviewing training awareness programs, security policies, regulations set by stakeholders, and information technology systems. This actively demonstrates and enables Fullsoft to determine security gaps and vulnerabilities that were not encountered previously and compares the current IT security posture against the defined objectives and goals, allowing security professionals to triage possible risks within those gaps. Nevertheless, regulations are applicable depending on the location, industry, and data types involved, Fullsoft will likely enforce GDPR, PCI DSS, or CCPA.

Gaps and Weaknesses

It is not only important to execute security controls but also to regularly audit them against new regulations; along with conducting vulnerability assessments, and updates to policies in Fullsoft's infrastructure to ensure they remain effective. Prioritizing gaps to safeguard the most vulnerable assets first by performing remediation on the severity, likelihood, and potential impact on sensitive data is required to close gaps that Fullsoft may bear. This tailored approach increases security ROI and decreases any possible exposures. Continuously updating components of Fullsoft's infrastructure must be a dynamic process that takes many assets into

account. These and many other procedures can be accomplished with the support of tools such as Nessus, OpenVAS, Wireshark, Nmap, Burp Suite, and many more. Data-driven and risk-based approaches to improve security controls can be **user authentication**, **separation of duties**, **system monitoring**, **access control mechanisms (RBAC)**, **software configuration management**, **data loss prevention (DLP)**, or **data encryption** which are only a few that Fullsoft can take advantage of.

Analysis

Furthermore, it is substantial to perform a detailed analysis that exhibits the weaknesses found and splits security processes into security controls that can be applied to Fullsoft's most fundamental systems to designate and enact remedial measures to meet policy compliance. The granular analysis of weaknesses allows for categorization to segment actionable controls made specifically for Fullsoft's core systems. Fullsoft must also hold communication to demonstrate the gap analysis findings, action plan details, and progress updates to all relevant stakeholders, ensuring alignment.

Post Analysis Activity

A final report must define the current status, outline a feasible timeline for achieving the main goal, estimate the actual costs of reaching the goal, and specify the change controls needed. Fullsoft must continuously monitor the implemented controls, adjust the plan for arising threats, and adapt to maintain progress toward closing new gaps. Fullsoft will operate collaboratively to seamlessly integrate the gap analysis results and action plan into existing security processes and workflows, minimizing disruption and maximizing efficiency. It is vital to also present clear metrics and data-driven insights showcasing the gap analysis' impact on security posture improvement, risk mitigation, and overall compliance. Finally, security professionals should

actively pursue and enforce further enhancements to security controls, policies, and processes based on evolving best practices, industry standards, and evolving threats.

Gap Analysis Plan

As Fullsoft is a large company, NIST's SP such as the RMF (part of NIST SP 800-30 for Risk Assessment) or CSF is great for a company that has begun securing its assets for the first time.

1. **Research an applicable framework**, "Understand the CSF core" (Koumi et al., 2024).
    a. Define a framework that fits with Fullsoft's.
        i. How much time will be used?
        ii. How many resources are needed?
        iii. What will be the costs for executing the framework?
    b. NIST SP 800-30 along with RMF which is widely available and used.
2. **Set objectives and goals**, "Define your scope and context" (Koumi et al., 2024).
    a. Base Fullsoft's goals on its intellectual property which must be confidential.
        i. How will NIST support Fullsoft's intellectual property? (Proprietary Software).
        ii. Are the objectives and goals focused on the software that Fullsoft is trying to protect?
3. **Define an assessment of the current state** "Establish your current" (Koumi et al., 2024).
    a. Establish a baseline of Fullsoft to compare against a future state.
        i. What is Fullsoft doing correctly or incorrectly?
        ii. Is the current environment functional?
    b. Evaluate processes, regulations, and policies with stakeholders.

   c. Set a clear view of current weaknesses in Fullsoft’s infrastructure.
   d. Specify Fullsoft’s current compliance adherence, security controls, best practices, regulations, logical assets, physical assets, etc.

4. **Identify gaps and weaknesses**, “ Identify and prioritize your gaps” (Koumi et al., 2024).
   a. Triage gaps to protect the most vulnerable assets first.
   b. Update or renew the previously mentioned; compliance adherence, controls, practices, regulations if necessary, etc.
   c. Is data properly protected while in rest, transit, or use with Fullsoft's workstations?
5. **Formulate a detailed analysis**, “Develop and implement your action plan” (Koumi et al., 2024).
   a. What are the specific steps that Fullsoft needs to perform?
   b. Conduct the transition of security controls.
   c. Communicate the plan with stakeholders.
6. **Analysis examination and report**, “Here’s what else to consider” (Koumi et al., 2024).
   a. Assess, monitor, and adjust the implementation of the gap analysis.
   b. Ensure the proper transition of the gap analysis takes place efficiently.
   c. Demonstrate the outcome of the gap analysis.
   d. Are there additional improvements?

References

Graul, D., & McDonald, T. (n.d.). Department wide gap analysis & establishing a tier 2 information ... - CSRC. https://csrc.nist.gov/CSRC/media/Projects/Forum/documents/aug-2016/tues1230_pbgc_tier2-program.pdf

Kim, D., & Solomon, M. (2023). *Fundamentals of Information Systems Security*. Jones & Bartlett Learning.

Koumi, D., Bhatt, A., J., C., & Janet, W. (2024, January 13). *What are the best practices for conducting a gap analysis based on the NIST cybersecurity framework?*. How to Conduct a Gap Analysis with NIST Framework. https://www.linkedin.com/advice/1/what-best-practices-conducting-gap-analysis

YouTube. (2023, November 1). *Gap analysis - comptia security+ sy0-701 - 1.2*. YouTube. https://www.youtube.com/watch?v=cuTVyyS5C7M