ISM6124.300S2 ADVANCED SYSTEMS ANALYSIS AND DESIGN

Revised SRR, PDR

TOPIC - System Analysis and Design for Data Security

Team Fantastic Four

Nikhil Reddy Kotwal

Simran Agichani

Yeshwanth Kumar Lekkala

Neha Sapare

Contents:

🡪Requirements

🡪Stakeholders

🡪Preliminary design review

🡪Scope

🡪WBS

🡪SOW

🡪Gantt chart

Requirements

A Functional Requirements Document (FRD) or a Computer Software Configuration Item (CSCI) is a detailed specification that outlines the functional requirements and constraints of a software system. Here is a high-level outline of what a FRD or CSCI for a business problem related to security breaches and data loss might include:

• Access control: The system must have a robust access control mechanism to manage user permissions and prevent unauthorized access to sensitive data.

• Monitoring and logging: The system must have monitoring and logging capabilities to track and record all user activity and detect any potential security breaches.

• Data backup: The system must support regular data backups to minimize the impact of data loss.

• Data recovery: The system must have a reliable data recovery solution to restore lost or corrupted data.

Non-functional requirements (NFRs) are requirements that define the quality attributes of a software system, such as performance, security, usability, and maintainability. Here are some common NFRs for a business problem related to security breaches and data loss:

• Security: The system must protect sensitive data from unauthorized access and prevent security breaches from occurring. This may include requirements for encryption, authentication, access control, and monitoring and logging.

• Data backup and recovery: The system must have a reliable backup and recovery solution to minimize the impact of data loss. This may include requirements for data backup strategies, recovery time objectives, and recovery point objectives.

• Usability: The system must be easy to use and understand, even for non-technical users. This may include requirements for user-friendly interfaces and clear and concise documentation.

• Reliability: The system must be reliable and available when needed. This may include requirements for system uptime and response time.

• Scalability: The system must be able to handle increased workloads and changing requirements over time. This may include requirements for system performance and capacity.

• Maintainability: The system must be easy to maintain and upgrade over time. This may include requirements for system documentation and support.

Stakeholders

• Business Owners and Management: They are responsible for ensuring the security of the organization's data and are ultimately accountable for the financial and reputational impact of a security breach.

• IT and Security Teams: They are responsible for implementing and maintaining the security systems and processes to prevent security breaches and data loss.

• Customers: They provide the sensitive data that is being protected and are the ultimate victims of a security breach if their personal information is compromised.

• Regulators: They set the standards for data protection and enforce laws and regulations that businesses must adhere to.

• Shareholders: They are invested in the success of the business and have a vested interest in the security of its data.

• Business Partners: They may have access to the organization's data and could be a source of a security breach.

• Insurance Providers: They may offer coverage for financial losses related to security breaches and data loss.

• Legal Teams: They may be involved in legal proceedings related to a security breach and data loss.

Preliminary Design Phase Introduction

Once the requirement gathering, classification and identification of stakeholders is complete one can begin the make or buy decision which is done after evaluating strategic and logistical considerations.

Strategic considerations deal with high level view of the organization which leads to the ultimate question about in-sourcing or outsourcing. As it’s a matter of security, the main purpose of the system is too critical to be leveraged for any risks. The access to the data should be minimal to avoid any security breaches and data loss. Hence, we want to perform it and maintain ourselves and not outsource it.

Logistical considerations deal with the organization’s specific methods for accomplishing its goals and objectives. One of them is span of control, which is a ratio that is supposed to be less for our system as it’s based on less access division. Therefore, for our system, build decision would seem to be more appropriate.

Scope

A project’s scope is found by understanding “what needs to be done to complete it”. The scope is defined to further clarify the contents of the requirements and improve the granularity of the system’s component parts that need to be built and supported. The two aspects are defining activities and their sequence. The work breakdown structure (WBS) is the supporting document for the definition of activities. The main supporting document for the sequence of activities is the Gantt chart.

Work Breakdown Structure

Diagram

Description automatically generated

SOW

A statement of work (SOW) is the document that tracks a narrative description of what is detailed in the WBS and traces directly to the CSCI. For our system the detailed narrative would be as follows:

**Fire wall:** A firewall is a crucial component of network security that helps establish security policies, deploy network security, and create zones with specific IP addresses. The firewall configuration is tested before deployment to ensure it meets the security policies. The implementation of a firewall helps in securing the network from unauthorized access and cyber threats.

**Intrusion Detection System:** An Intrusion Detection System (IDS) is a security tool that helps detect and prevent unauthorized access to a network. The IDS has features to turn on intrusion prevention, set the enforcement mode, schedule recommendation scans, and report or collect violations using Security Event Manager (SEM). The IDS monitors network traffic and identifies potential security threats, alerting administrators to take appropriate action to prevent security breaches. The IDS is an essential component in securing a network from potential intrusions and cyber-attacks.

**Encryption and Access Control:** Encryption and access control are important security measures to protect sensitive information. Encryption is the process of translating sensitive information into a code to prevent unauthorized access. Access control is achieved by using passwords or one-time passwords (OTP) for authentication and limiting access to authorized individuals using lists. By implementing encryption and access control, organizations can ensure that only authorized users have access to sensitive information and prevent unauthorized access, thus enhancing the overall security of the network.

**Regular updates:** Regular updates are an important aspect of maintaining network security. This involves regularly checking for antivirus and software updates, updating to the latest versions, and changing passwords at regular intervals. Keeping software up-to-date helps ensure that any vulnerabilities are fixed, and changing passwords helps prevent unauthorized access. Regular updates help ensure that the network is protected from potential security threats and vulnerabilities and that sensitive information remains secure.

**Employee Training:** Employee training is an important aspect of maintaining network security. This involves educating employees about security protocols and best practices. Employee training can be done through in-person training sessions, online courses, creating surveys, and raising awareness. By providing employees with the necessary knowledge and skills to identify and prevent security threats, organizations can reduce the risk of security breaches. Regular employee training helps ensure that the network remains secure, and that sensitive information is protected.

Gantt Chart

Developed by Henry Gantt, it is a scheduling tool visually displayed as a bar chart. It is an industry standard for planning, monitoring, and controlling the progress of a project. The chart is developed from the WBS and displays the elements as milestones, activities, dependencies, slack, and the critical path.

Chart

Description automatically generated with low confidence

Graphical user interface, table

Description automatically generated