**Unit 8**

**Activity 2**

**What are the main risks that the authors identify? How do these fit into the traditional SDLC model?**

In the article by Verner et al. (2014), the researchers investigated the Global Software Development System Literature Reviews, which focused on discovering risks and their mitigation strategies. They discovered Global Software Development risks and their mitigation strategies in their search. They found about 85 risks. The major risks identified in this research were: project management, software development, outsourcing rationale and human resources. Among the categories of risks, project management appeared to be the largest. Outsourcing rationale risks were rated the highest considered under the preliminary study. On several occasions, the risks were singled out by a single System Literature Review (Verner et al., 2014).

In the SDLC model, risk management is to help in the documentation of previously known risks and prioritize them. It is also used in establishing processes and duties for risk management in the preliminary analysis stage. In the feasibility study stage, the risks in the project management, which was identified as the largest, can be related to mistakes in project scope, improper estimation of cost, resources, and time. Unachievable Budget: As previously mentioned, a faulty budget estimation can result in a project going bankrupt initials of the SDLC. Appropriate knowledge of the effort, time invested, and resources is directly tied to accurate budget estimation. An unrealistic calendar puts pressure on developers to deliver projects on time due to inaccurate time estimates. As a result, the project's overall quality suffers, and the system becomes less secured and more susceptible. Inadequate resources, which in some cases, the technology and tools provided are not up to date to satisfy project needs, or the available resources people, tools, and technology are insufficient to accomplish the project. In any situation, the project will be delayed, and in the worst-case scenario, it will fail.

Project managers must know what the project is designed to accomplish, which critical features, which functionalities are compulsory, and which ones might be considered optional. Project failure may result from a lack of understanding of the system.

**Which of the frameworks discussed in the Unit 7 lecture cast would you use to capture and categorize the risks?**

The risks can be categorized under Risk Management Process. There are a variety of risk-specific frameworks available, including some that reference or include risk in some form.The NIST Risk Management Framework (RMF) is a seven-step method that every company can use to handle privacy and security risk for institutions. It also links to a suite of NIST guidelines and standards to help organizations implement risk management programs that satisfy the Federal Information Security Modernization Act (FISMA) demands. The Risk Management Framework has outlined steps that will help mitigate the risks in the SDLC. The steps are as follows:

Preparation: it helps execute critical efforts to assist all company levels in preparing to handle security and privacy threats utilizing the RMF. The company's risk management strategy is defined, essential risk management roles are identified, and established risk tolerance. A wide risk assessment created and executed an organization-wide plan for continuous monitoring.

Categorization: these steps assist in determining the negative impact on systems and the data processed, stored, and communicated by such systems to influence the institutional Risk Management Processes and duties. System features are documented, system security classification and information are done, and categorization determination is reviewed or approved by approving officials.

Selection: this phase selects, customizes, and documents the measures required to protect the system or business in a risk-adjusted manner. It also controls the designated measures as hybrid, system-specific and common. It also results in measures allocated to specific components of the system. The selection process ensures that the privacy and security plan are approved.

Implementation: the implementation process is where the measures and records are deployed. The process seeks to implement security plans and update them to reflect measures previously implemented.

Assessing: the phase helps determine whether the measures are correctly implemented, working as intended, and giving the right results to achieve privacy and security requirements for the organization. The outcomes of this process are the development of security assessment reports and plans, development of a plan of milestones and action, approval of

Authorization: this step is to be accountable where the top official determines whether the security risks are based on the system operations or acceptability of the common measures. The authorization ensures that the response ae provided and determined.

Monitoring: under this step, continuous monitoring is done on the implementation of the measures. The step helps maintain the continuing awareness on privacy and security state of the organization or system back the decisions on risk management.

**Add a risk and a suggested mitigation to the module forum**

In the process of software development in SDLC, security will always be an issue. The fundamental cause of such risks is frequently a lack of competence and privacy and security considerations during the creation of systems. Risk mitigation techniques were previously implemented in the Systems Development Life Cycle in an unstructured manner, resulting in both under and over-investment in development management. Many firms claim to adopt a risk-based strategy that involves cost-effective risk mitigation levels proportional to the company's risk tolerance (Bardin, 2010). Security architecture, the organization within the Systems Development Life cycle, and a robust coding curriculum and training should all be used in the attempt.

To mitigate this risk, Security organizations must design a repeatable and quantifiable process that allows Systems Development efforts to meet company goals for error-free, low-vulnerability systems. Although the procedure is not without defects, the development team should be aware of applying relevant controls optimally throughout the SDLC. Confidentiality protections, such as encryption, should be used both at transit and at rest on every critical data, for example, Personal Identifiable Information(PII), processed by the system, according to the Security Architecture. Furthermore, architecture necessitates data integrity safeguards, like security management data, whose modifications would expose the system to threats (Bardin, 2010).

**Reference**

Bardin, J. (2010). Risk, Architecture and Development in the SDLC. *The Brave New World Of Infosec*

Verner, J. M., Brereton, O. P., Kitchenham, B. A., Turner, M., & Niazi, M. (2014). Risks and risk mitigation in global software development: A tertiary study. *Information and Software Technology*, *56*(1), 54-78.

Anton, S. G., & Nucu, A. E. A. (2020). Enterprise risk management: A literature review and agenda for future research. *Journal of Risk and Financial Management*, *13*(11), 281.