It is essential as a security expert to be able to evaluate potential risks within a security infrastructure in order to position security controls/countermeasures. The system design document (SDD) describes the high-level system design and the low-level detailed design specifications from which a system is built. As part of the security development team, this document provides the information necessary for designing and implementing a system.

Refer to the "System Lifecycle Framework Template," located in the topic Resources, as well as your assignments from CYB-525, and create a 1,250- to 1,500-word system design document and the overall security architecture structure diagram for your current organization.

**Part 1: Security Architecture**

Address the following:

* Identify and define all hardware and software devices, and the different types of sensitive data the organization will store.
* Explain the organization's technical requirements in compliance with all devices and services internally and externally that could be a potential target for cyberattacks.
* Describe in-depth how the security controls and services are positioned, and how they relate to the overall systems architecture to prevent attacks.
* Demonstrate restricting access, layering security, employing authentication, encrypting storage, and automating data security by including the full scope of policy, procedural, and technical responsibilities in the IT infrastructure.
* Apply knowledge to effectively manage a security program.
* Assess the effectiveness of a security program.

**Part 2: System Design**

Address the following:

* Describe the design goals and considerations, and articulate threat modeling, providing a high-level overview of the security architecture.
* Describe the security baselining and the data design associated with the system, and explain the human-machine interface and operational scenarios.
* Design a high-level system diagram that further deconstructs into low-level detailed design specifications for each system component, including hardware, internal communications, software, system integrity controls, and external interfaces, all of which are a part of the program monitoring and control.
* Describe the importance of secure software, and the programming practices, development processes, and methodologies that lead to secure software.

**Note:** Since this course is the culmination of the Business Continuity Plan, students may utilize or adapt any of their previous assignments from earlier classes in the program for assignments in this course.

While APA style is not required for the body of this assignment, solid academic writing is expected, and documentation of sources should be presented using APA formatting guidelines, which can be found in the APA Style Guide, located in the Student Success Center.  An abstract is not required.

This assignment uses a rubric. Please review the rubric prior to beginning the assignment to become familiar with the expectations for successful completion.

You are not required to submit this assignment to LopesWrite.