To help manage and operate an ongoing security program in an organization, the information security team must adopt a security framework that serves as a guide for the development and implementation of the security program.

Prior to beginning this assignment, view the videos "1-1 Introduction to CYB-535" and "1-2 Introduction to Topic One," located in the topic Resources.

Use the company from your Business Continuity Plan (BCP) – Phase 1, developed in CYB-515. In a 750- to 1,000-word summary, address the following:

Provide a basic description of the company which includes:

* Mission statement
* Web applications
* Servers
* Departments
* Routers and switches
* Remote access
* Wireless communication
* Firewalls
* Demilitarized zone (DMZ)

The NIST Cybersecurity Framework (CSF) is a list of guidelines and practices designed to help organizations better manage their security programs. It rests on various industry best practices and standards like ISO 27001 and the Control Objectives for Information and Related Technologies (COBIT) 5 (refer to the topic Resources to learn more about these standards). This framework discusses critical security controls that can be tailored and customized to your organization's unique needs. Your task as a part of the security team in your organization is to prepare and present a report to upper management that discusses the following steps:

* Describe how you would introduce the NIST CSF critical security activities into your organization.
* Determine current/recent risks or dominant categories of threats to information security.
* Develop system-specific plans for the protection of intellectual property.
* Apply the security model to information security management to protect the organization from being compromised by unauthorized users.
* Determine appropriate implementation of the management of access control mechanisms that would apply to ensure information is protected against unauthorized users.
* Outline and explain the roles of the following personnel in the planning and managing of this security plan by examining C-level functions that impact cybersecurity:  
  - Board of Directors  
  - Senior Management  
  - Chief Information Security Officer (CISO)  
  - IT Management (CIO, IT Director, etc.)  
  - Functional Area Management  
  - Information Security Personnel  
  - End Users

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.

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

You are required to submit this assignment to LopesWrite. A link to the LopesWrite technical support articles is located in Class Resources if you need assistance.