A major goal of a compliance risk assessment framework is to determine the company's legal and reputational risk exposure in regard to adhering to laws and regulations, as well as all internal company policies and standards of conduct.

Build on to your "Business Profile" from Topic 1 and the "Challenge Your Hacking Skills," assignment from CYB-610 by writing a 1,000- to 1,250-word report on compliance and security governance that includes the following:

**Cybersecurity Risk Assessment:**

Interpret risk assessments, gap analysis, and current cybersecurity trends to formulate a cybersecurity governance strategy that establishes mitigation plans for future challenges to achieve security . Describe the likelihood of risks occurring and the resulting impact. Identify threats to, and vulnerabilities of, those systems and assets based on various risk analysis methodologies. Express risks both internally and externally. Determine the acceptable level of risk (risk tolerance) with respect to technology, individuals, and the enterprise.

**Privacy Risk Management:**

Define the role of project/program management and process management. Describe how the business is integrating the compliance with applicable privacy laws and regulations, prioritizing and measuring progress with security policies. Analyze the ethical implications of cybersecurity policies and regulations put in place to protect the confidentiality, integrity, and availability of your organization's intellectual property.

**Compliance Gaps:**

Summarize the various type of audits that should be effectively performed in order to keep a consistent measure of risk. Determine what type of gap analysis should be performed in order to properly identify the security elements and variables within the environment that pose the most risk. Formulate a cybersecurity governance strategy that establishes mitigation plans to achieve security objectives.

**Security Measures:**

Apply your knowledge to develop a security program, identifying goals, objectives, and metrics, and make the necessary modifications for the system security plans.

**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.