***Case Study: Problem 1***

*JCI has hired you, a consultant, to assist them with a comprehensive look at their database and application security environment. After an initial meeting with the president and chief information officer (CIO), it was determined that your first deliverable will be twofold. First, you will identify the types of information and data processed by the company, and second, you will look at project life cycles for systems within the company and outline what security measures should be taken at each phase.*

***Task 1***

*Create the shell document for the final project deliverable that you will be working on throughout the course. As you proceed through each assignment, you will add content to each section of the final document to gradually complete the final project delivery. Appropriate research should be conducted to support the analysis in your plan, and assumptions may be made when necessary.*

*The overall Data and Applications Security Impact Analysis and Mitigation Report project will consist of the following deliverables:*

* ***Section 1: Project Outline and Requirements***
* + *Give a brief description of the company (can be hypothetical) where the Data and Applications Security Impact Analysis and Mitigation Report will be implemented. Include the types of information and data that are processed by the company, the company size, location(s), and other pertinent information.*
* ***Project Life Cycle Security Measures***
	+ *Give a summary of the security measures to be taken at the planning, requirements, design, development, integration and testing, and installation and acceptance phases of the project life cycle to include the following:*
		- ***Planning phase:****Identify what work products the team will have that will change, or are likely to change, and the functional relationships between those products.*
		- ***Requirements phase:****Identify the requirements and the functional software verifying the identity of a user. Provide any requirements that are applicable to your cryptographic module. FIPS PBU140-2 Security Requirements for Cryptographic Modules can be used as a guideline.*
		- ***Design phase:****Describe how the design team ensures that the software component has trusted modules.*
		- ***Development phase:****Describe how developers will ensure that the application being developed for the cryptographic algorithm will be secure and protective of sensitive data.*
		- ***Integration and test phase:****Identify what will be tested during this phase and the general integration and test procedures that will be used.*
		- ***Installation and acceptance phase:****Identify the purpose of the installation and acceptance phase for both the user and the organization.*

* ***Section 2: Security Vulnerability Assessment***

*·       you will need to identify the Security Vulnerability Assessment to be done for the development phase of the life cycle.*

* *For the development phase of the life cycle, identify software vulnerabilities, associated poor programming practices, and the overall impact that they have on security with your selected organization.*
* *Identify best practices for fixing vulnerabilities and insecure interactions as introduced by poor coding.*
* *Provide a conclusion to summarize the importance of correcting the current vulnerabilities and programming practices.*
* *Update your table of contents before submission.*
* ***Section 3: Virtualization Security Impact***

*·       The next step to be completed is to perform the Virtualization Security Impact Analysis to identify the impact of moving an organization to virtualization.*

* *Provide an impact analysis that identifies the impact of moving an organization’s applications and databases to virtualization. Identify how this move impacts network security.*
	+ *Include the services being implemented in the virtualization solution.*
	+ *Include the strategies needed to mitigate security vulnerabilities that are associated with the organizational virtualization effort (e.g., current virtualization security vulnerability and security risks related to hypervisor security, host or platform security, and securing communications).*
	+ *Include the configuration management policies and practices that are applicable to the virtualization security implementation.*
* ***Section 4: Cloud Computing Security***
* *Identification of security risks to be addressed in the cloud computing environment:*
	+ *Operating system and other infrastructure complexity*
	+ *Unauthorized user access*
	+ *Increased administrator roles*
	+ *Legal compliance*
	+ *Issues related to programmer service mapping to the cloud*
	+ *Accesses to services moved to the cloud*
* *Describe the application that is being released into the cloud computing environment and how this affects security from a standpoint of network communications, system configuration, security controls, and user responsibilities.*
* *Describe the migration of corporate resources to various types of clouds, such as the private, public, hybrid, and community clouds, and the associated deployment model.*
* *Describe how services are related to cloud computing (e.g., software, platforms, and infrastructure services).*
* *Describe how organizations are placing controls and access policies on their data to control accesses to data and their locations on servers and off-site data locations.*
* ***Section 5: Risk Mitigation Strategies for Applications and Databases***
* *Provide a Word document of 2–3 pages that is delivered as a final section to your report, expanding on the following critical activities that are needed to create the Risk Management Framework:*
	+ *Risk Management of Software from a Business Perspective*
		- *Creates a basis for understanding what software risks are critical; current business goals, operational, and technical priorities; circumstances of taking certain business actions must be identified and understood*
	+ *Business and Technical Risk*
		- *Identification of what risks financially affect which organizational goals; reputation, liability concerns, and increased development cost; business and software risks must be quantified*
	+ *Risk Prioritization*
		- *Determines which business goals are critical or important and which technical risks may affect business operations*
	+ *Risk Mitigation Strategy*
		- *Strategy takes into account time, resources, likelihood of operational success, and overall impact; involves metrics and validation procedures to ensure the risks are mitigated*
	+ *Repair Problems With Architecture, Requirements, and Design*
		- *Involves the study of open risks, evaluating quality metrics, and judging progress against any existing risks*