**Assignment Instructions**

Select an organization that you would like to develop an IT governance strategy for, using ISO 27001, Information Security Management System (ISMS). You can find ISMS on the Internet or in this unit’s reading. The organization should be one you are familiar with from having worked there.

In your paper, include the following:

1. Define and discuss the ISO 27001 Information Security Management System in terms of the Deming Cycle of continuous improvement of Plan-Do-Check-Act (PDCA)
2. Brief description of the organization and type of business engaged in.
3. High level information security policy that defines management’s overall objective for information security as it relates to business requirements and relevant laws and regulations.
   1. Information security direction for the organization
   2. Information security objectives for the organization
   3. Information on how the organization will meet contractual, legal, and regulatory requirements
   4. A statement of commitment to continuous improvement of the ISMS.
4. High level risk assessment (for purposes of this paper, discuss the top 3-4 risks only)
   1. Define a risk management framework that will be used
   2. Identify risks and describe the risk
   3. Analyze and evaluate the risks in terms of severity and impact
5. Statement of Applicability
   1. Identify selected controls to address identified risks (again only the top 3-4 risks)
   2. Explanation of why these controls were selected
6. Conclusion paragraph

This is a short version of an IT governance strategy but will provide a good understanding of the elements that must be included for this ISO 27001 ISMS.

**Assignment Requirements**

1. The paper should be 4 pages.
2. Use Times New Roman 12 pt. font.
3. Use APA formatting for paper, citations, and three or more references.
4. Be sure to cite your sources and provide the appropriate three or more references.