

## SUBDOMAIN 427.3 - SECURITY POLICY & STANDARDS

**Competency 427.3.4: Certifications and Accreditations** - The graduate identifies and discusses the Information Assurance certification and accreditation (C&A) process.

---

### Introduction:

The National Institute of Standards and Technology (NIST) replaced the former NIST Special Publication 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems* with NIST Special Publication 800-37 Revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*. The NIST document changed from a certification and accreditation framework to a risk management framework because information security management systems should be regularly reviewed, updated, and maintained. It makes more sense to follow a security life cycle approach (continuous monitoring) versus a single one-time static certification/accreditation approach.

For this task, you will be using NIST Special Publication 800-37 Revision 1, *Guide for Applying Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* and the attached "Healthy Body Wellness Center Risk Assessment" case study.

You have been hired to apply the NIST's risk management framework to the Healthy Body Wellness Center's information systems. You know that the organization has recently had a risk assessment completed that includes recommendations for implementing security controls and mitigating risks. In your new role, a team of people will be assigned to help you with the task. The first job you are tasked with is creating a to-do list for the specific tasks outlined in each of the six steps in the risk management framework (RMF).

### Task:

- A. Discuss key elements that need to be addressed as part of the risk management framework by completing the attached "RMF To-Do List."
- B. Create a white paper that compares the ISO 27002, COBIT, NIST, and ITIL frameworks by doing the following:
  - 1. Discuss how *each* framework is most commonly used.
  - 2. Analyze the purpose of *each* framework design.
  - 3. Evaluate the strengths of *each* framework.
  - 4. Evaluate the weaknesses of *each* framework.
  - 5. Discuss the certification and accreditation process for the frameworks.
  - 6. Discuss when you would choose to use *each* framework (e.g., ISO 27002 versus COBIT, NIST, or ITIL).
- C. When you use sources, include all in-text citations and references in APA format.

*Note: When bulleted points are present in the task prompt, the level of detail or support called for in the rubric refers to those bulleted points.*

*Note: For definitions of terms commonly used in the rubric, see the Rubric Terms web link included in the Evaluation Procedures section.*

*Note: When using sources to support ideas and elements in a paper or project, the submission MUST include APA formatted in-text citations with a corresponding reference list for any direct quotes or*

*paraphrasing. It is not necessary to list sources that were consulted if they have not been quoted or paraphrased in the text of the paper or project.*

*Note: No more than a combined total of 30% of a submission can be directly quoted or closely paraphrased from sources, even if cited correctly. For tips on using APA style, please refer to the APA Handout web link included in the General Instructions section.*

**File Attachments:**

---

- 1. Task 4 Healthy Body Wellness Center Risk Assessment**
- 2. Task 4 RMF To-Do List**