

2 Management Controls

Describe the management-level approach to controlling security for the system. This includes risk assessment processes, risk review, and the behavioral expectations of all individuals who work within the system.

2.1 Risk Assessment and Management

Describe the risk assessment methodology used to identify the threats and vulnerabilities of the system. List the group that conducted the assessment and the date(s) the review was conducted. If there is no system risk assessment, include a milestone date (month and year) for completion of the assessment.

2.2 Review of Security Controls

Identify any independent security reviews conducted on the system in the last [X] years. Include information about the type of security evaluation performed, who performed the review, the purpose of the review, the findings, and the actions taken as a result.

2.3 Rules of Behavior

At least 1 Rule of Behavior must be prepared for each system. Ensure that these rules are made available to every user prior to the user accessing the system; attach a signature page to acknowledge receipt.

The rules clarify roles, responsibilities and the expected behavior of all individuals with access to the system. It should state the consequences of inconsistent behavior, non-compliance, and appropriate limits on interconnections to other systems.

Attach the rules of behavior to the Appendix and reference the appendix number here.

2.4 Planning for Security In the Life Cycle

Although a security plan can be developed at any point in the life cycle, the recommended approach is to design the plan at the start of the life cycle. In some cases, the system may be in several phases of the life cycle at any one time; for example, one life cycle phase may include the disposal phase, and other may address the initiation and acquisition phase; and a final phase may address operations and maintenance.

Identify which phase(s) of the life-cycle the system, or parts of the system, are in. Describe how security has been handled during each of the listed life cycle phases:

- Initiation
- Development/acquisition
- Implementation
- Operations/Maintenance
- Disposal