

## Minimum Requirements to Authorize a System for Operation

Management authorization must be based on an assessment of management, operational, and technical controls. Since the security plan establishes the system protection requirements and documents the security controls in the system, it should form the basis for the authorization. Authorization is usually supported by a technical evaluation and/or security evaluation, risk assessment, contingency plan, and signed rules of behavior. Note: Some agencies refer to the technical evaluation and/or security evaluation as a certification review. Re-authorization should occur prior to a significant change in the system, but at least every three years. It should be done more often where there is high risk and potential magnitude of harm.

Below is the minimum security controls that must be in place prior to authorizing a system for processing. The level of controls should be consistent with the level of sensitivity the system contains.

- Technical and/or security evaluation complete
- Risk assessment conducted
- Rules of behavior established and signed by users
- Contingency plan developed and tested
- Security plan developed, updated, and reviewed
- System meets all applicable federal laws, regulations, policies, guidelines, and standards
- In-place and planned security safeguards appear to be adequate and appropriate for the system
- In-place safeguards are operating as intended

(NIST Special Pub 800-18/Guide for Developing Security Plans for IT Systems, Section 4.5 Authorize Processing)