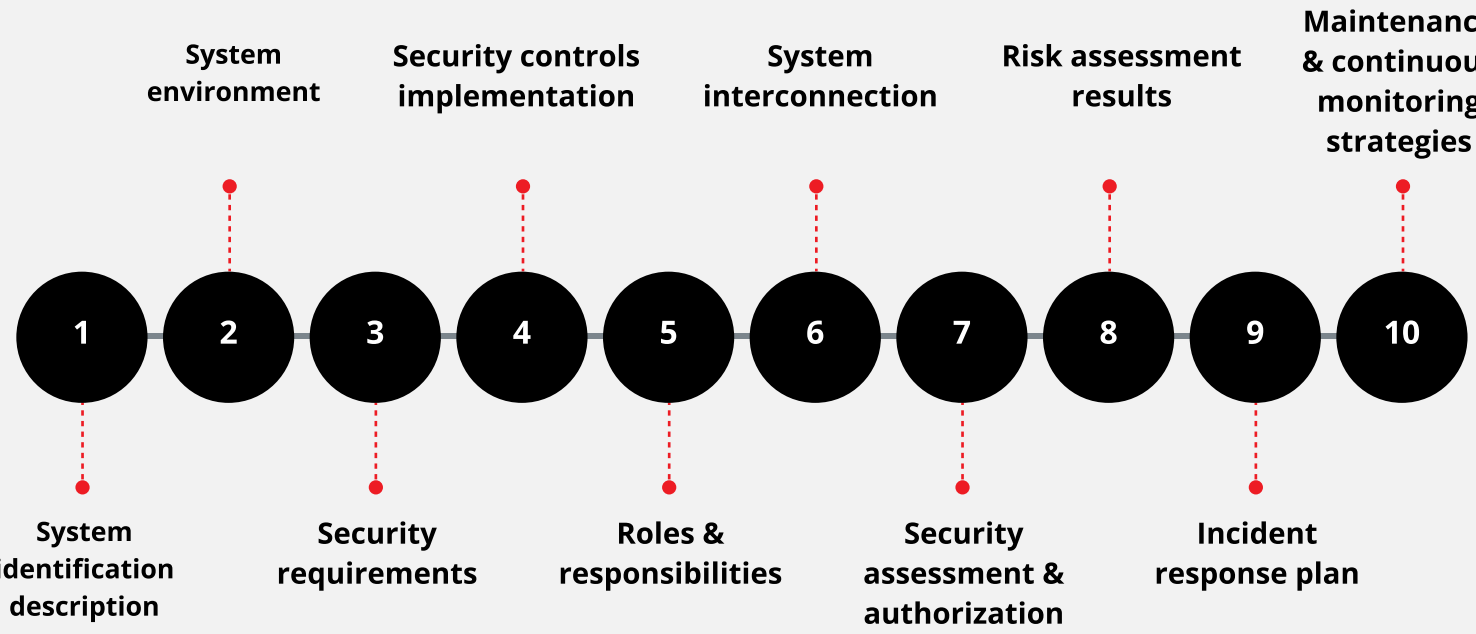
REDSEAL

System Security Planning with RedSeal

In high-security environments like the DoD and the Intelligence Community, the System Security Plan (SSP) is critical for ensuring that systems handle sensitive national security data appropriately. It helps in achieving and maintaining the authorization to operate (ATO), which is mandatory for systems that process, store, or transmit classified information. The SSP ensures all stakeholders are aware of the security features of the system and understand their responsibilities in maintaining its security integrity.

The SSP is not only a compliance document but also a dynamic tool used for ongoing security management and decision-making, essential for maintaining the stringent security requirements demanded by the DoD and Intelligence Community.

Phases of SSP



Key aspects of SSP

Step	RedSeal Function	Benefit
System identification	Provides detailed network mapping and visualization capabilities.	Helps define the system boundary by identifying all network devices and connections, ensuring a comprehensive description of the system.
System environment	Models both the physical and virtual aspects of the network environment.	Offers a clear view of how the system operates within its environment, including how data flows across the network and external interactions.
Security requirements	Integrates with compliance frameworks and checks against security policies.	Ensures all security controls meet specific requirements outlined in relevant security standards and regulations.
Security controls implementation	Automatically maps and validates security controls against industry standards like NIST SP 800-53.	Helps document the implementation details of each security control within the network, including configurations and the effectiveness.
Roles & responsibilities	Does not directly manage roles and responsibilities but provides documentation and reporting that supports role definition.	Helps define the scope of responsibility for network security, detailing responsibility for managing and operating specific security controls.
System interconnection	Identifies and documents all network connections and interdependencies.	Assists in accurately describing each interconnection, including security measures and data flow between systems.
Security assessment & authorization	Facilitates security assessments by providing comprehensive network visibility and risk analysis.	Enhances the security assessment process, helping document current security state and changes needed for maintaining or obtaining ATO.
Risk assessment results	Conducts thorough risk assessments and prioritizes vulnerabilities.	Provides detailed insights into potential risks, helping to document current risks and previous assessments in the SSP.
Incident response plan	Models potential attack paths and simulates breach scenarios.	Supports development and documentation of system-specific incident response plans by identifying critical assets and potential attack vectors.
Maintenance & continuous monitoring	Offers continuous monitoring of the network's security posture and compliance status.	Helps document the procedures and technologies used for continuous monitoring and maintenance of security controls, ensuring the SSP remains up-to-date with the actual security posture of the system.

RedSeal significantly streamlines the process of SSP development and maintenance by providing critical data, insights, and automation capabilities. This support not only enhances the accuracy and effectiveness of the SSP but also reduces the manual effort required from ISSOs and ISSMs, allowing organizations to focus more on strategic security management tasks.

For more information on how RedSeal can support your System Security Plan, contact us today.