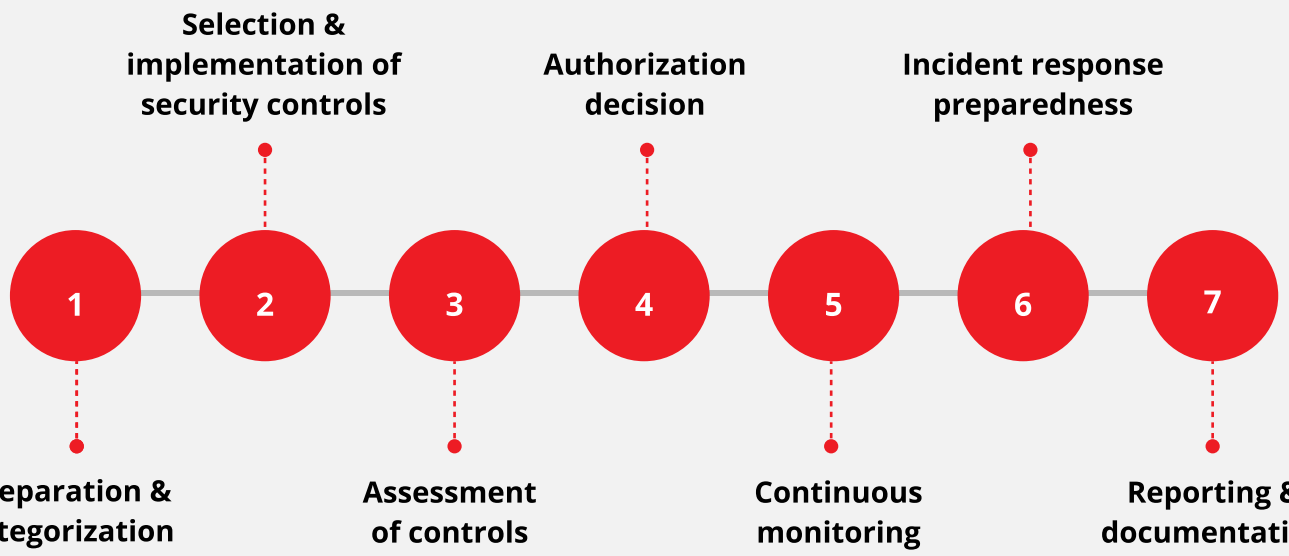
REDSEAL

Navigating the Authorization to Operate Process with RedSeal

The Authorization to Operate (ATO) is a critical component in the security architecture of the DoD and IC, ensuring that systems operate with a recognized and accepted level of risk. This process underscores the rigorous standards that these systems must meet to safeguard national security effectively.

RedSeal can significantly assist system owners, Information System Security Officers (ISSOs), and Information Systems Security Managers (ISSMs) in obtaining and maintaining an Authorization to Operate (ATO) for systems within environments such as the Department of Defense (DoD) and the Intelligence Community (IC).

Phases of the ATO process



© 2024 RedSeal. All rights reserved.

How RedSeal can support each phase of the ATO process:

Step	RedSeal Function	Benefit
Preparation & categorization	Assists in network discovery and asset identification, crucial for system categorization.	Ensures the system categorization reflects the real operational environment, helping to select appropriate security controls.
Segment & implementation	Provides insights into network vulnerabilities and security gaps.	Helps ensure the implemented controls are adequately addressing the identified risks, making the system more secure and compliant.
Assessment of controls	Facilitates continuous vulnerability assessments and compliance checks against security policies.	Provides detailed documentation and reports that can be used during the security control assessment phase.
Authorization decision	Offers comprehensive security metrics and risk scores that summarize the security posture of the network.	Enables AOs to make informed risk-based decisions regarding the ATO, supported by empirical data on the network's security readiness.
Continuous monitoring	Continuously monitors the network for changes that might affect security postures.	Helps maintain ongoing ATO compliance by ensuring that any changes or updates to the system do not introduce new risks.
Incident response preparedness	Simulates potential attack paths and prioritizes remediation efforts based on the risk to critical assets.	Enhances the incident response strategy, which is a critical component of the continuous monitoring and operational resilience required for ATO maintenance.
Reporting & documentation	Generates detailed reports and visualizations of network compliance, security postures, and risk assessments.	Reports are integral to the documentation required for ATO audits and reviews, providing clear evidence of compliance and proactive security management.

By leveraging RedSeal's capabilities, system owners, ISSOs, and ISSMs can effectively manage the lifecycle of an ATO—from initial authorization through continuous compliance monitoring. RedSeal's tools help streamline the process, reduce the complexity of compliance, and enhance the overall security posture of the systems, thereby supporting the critical requirements of ATO maintenance in high-security environments.

For more information on how RedSeal can assist navigating the ATO process for your organization, contact us today.

RedSeal, a leader in network exposure management, offers proactive insights to close security gaps in hybrid environments. It creates a network digital twin for comprehensive visibility and protection. Trusted by Fortune 1000 companies and U.S. military branches, RedSeal enhances operational efficiency, boosts productivity, and reduces business risk.
www.redseal.net | info@redseal.net | +1 408-641-2200 | 888-845-8169
© 2024 RedSeal. All rights reserved.