

CREDANT Solutions for FISMA Compliance

A strategic solution is essential for ongoing compliance and data protection



REGULATORY OVERVIEW

The Federal Information Security Management Act (FISMA) provides the framework for securing the federal government's information technology. All agencies covered by the Paperwork Reduction Act must implement the requirements of FISMA and report annually to the Office of Management and Budget (OMB) and Congress on the effectiveness of the agency's security programs. The reports must also include independent evaluations by the agency Inspector General.

The National Institute of Standards and Technology (NIST) develops and issues standards, guidelines, and other publications to assist federal agencies in implementing FISMA and in managing cost-effective programs to protect their information and information systems.

THE COMPLIANCE CHALLENGE

To promote the development of key security standards and guidelines, FISMA requires federal agencies to:

- › Develop an agency-wide security program, categorizing information and information systems by mission impact.
- › Implement and adhere to security configuration standards developed by NIST.
- › Select appropriate security controls for information systems.
- › Perform ongoing assessment and testing.
- › Conduct annual reviews on the effectiveness of the agency's information security and privacy programs, with results reported to the OMB annually.

Reporting to the OMB is a key element in demonstrating FISMA compliance. The report must contain proper evaluations of the effectiveness of the information security programs, including evidence that the agency has developed a coordinated strategy of addressing security threats.

If an agency implements a technology solution to raise their score in one year, they may score lower the following year if they fail to demonstrate how the solution fits into the agency's overall information security strategy.

CREDANT

CREDANT is the Trusted Expert in Data Protection. Founded in 2001, CREDANT enables organizations to control, manage and protect data on vulnerable laptops, desktops, PCs, Macs, smartphones and removable media devices.

CREDANT SOLUTION

CREDANT encryption management solutions ensure that encryption and security mandates are consistently and efficiently enforced – regardless of where the data resides.

ONLY CREDANT ENABLES ORGANIZATIONS TO:

- › Manage encryption and secure data across multiple endpoints from a common management platform
 - › Full Disk Encryption (FDE)
 - › Self-Encrypting Drives
 - › Policy-Based File/Folder Encryption
 - › Mobile Devices and Smartphones
 - › Removable Media
 - › Windows[®] BitLocker[™]
- › Create automatic audit trails that offer proof of end-to-end data security
- › Provide a transparent end-user interface that supports user productivity while keeping data safe
- › CREDANT provides you with a centrally-managed, highly scalable and architecturally flexible approach to manage all data endpoints. With CREDANT, organizations can:
 - › Help ensure data security, reducing the risk of insider or external attack
 - › Simplify and reduce the workload of maintaining compliance
 - › Provide confidentiality, privacy and auditing of data residing on any endpoint
 - › Integrate and manage multiple encryption solutions into a single management tool set