# FISMA COMPLIANCE

FISMA is part of the E-Government Act of 2002 introduced to improve the management of electronic government services and processes. It reduces the security risk to federal information and data while managing federal spending on information security.

## FISMA COMPLIANCE CHECKLIST

**Maintain Information System Inventory**

- Inventory must include an identification of the interfaces between each system and all other systems or networks.

**Categorize Information Systems**

- Information systems should be categorized according to range of risk levels.

**Maintain a System Security Plan**

- Develop and maintain a system security plan, which is a living document that requires periodic review, modifications, action plans, and milestones for implementing security controls.

**Utilize Security Controls**

- Apply baseline security controls to closely fit the mission requirements and operational environments. The controls must be documented in the System Security Plan.

**Conduct Risk Assessments**

- Assess and validate security controls to determine if any additional controls are needed to protect the organization's operations, assets, individuals, and other organizations.

**Certification and Accreditation**

- System controls must be certified to be functioning properly. Based on the results, the information system is accredited.

**Continuous Monitoring**

- Information systems are required to monitor a select set of security controls. Activities include security impact analyses, ongoing assessment of security controls and status reporting.