Overview:
- Determine security requirements for the state information system.
- Manage the technology life cycle by defining security roles and responsibilities, and integrating the risk management process.
- Follow change control procedures to ensure separate duties for development and test/production areas, and removal of test data before system is active.
- Develop applications based on secure coding guidelines to prevent coding violations.
- The acquisition process must include descriptions and requirements for security function and controls, security strength, security assurance and acceptance criteria.
- Administrator documentation for the state information system must describe user-accessible security functions, methods for user interaction, user responsibility in maintaining system security, and protection documentation in accordance with risk management.
- Perform configuration management during development, implementation and operation and document accordingly.
- Independent agents to verify the correct implementation of the security assessment plan and conduct penetration testing.

Purpose:
Establish adequate security controls for the acquisition and deployment of state information systems.

Why it’s important:
Implementing the right technology best meets the agency’s requirements and also follows federal and state regulations for encryption. Mitigates potential risks and vulnerabilities.

Target audience:
IT managers, finance managers, procurement team