

**SAM – INFORMATION SECURITY**  
**(Office of Information Security)**

**RISK MANAGEMENT**  
(Revised 6/14)

**5305.6**

**Policy:** Each state entity shall create a state entity-wide information security, privacy and risk management strategy which includes a clear expression of risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the state entity's risk tolerance, and approaches for monitoring risk over time.

The state entity's risk management strategy and methodologies shall be consistent with [NIST SP 800-30](#) and [NIST SP 800-39](#), and must include:

1. Risk assessments conducted at the three various levels of the risk management hierarchy, including:
  - a. Organizational level;
  - b. Mission/Business process level; and
  - c. Information asset level.
2. A risk assessment process to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks; including, but not limited to:
  - a. Risk associated with introducing new information processes, systems and technology into the state entity environment;
  - b. Accidental and deliberate acts on the part of state entity personnel and outsiders;
  - c. Fire, flooding, and electric disturbances; and,
  - d. Loss or disruption of data communications capabilities.

**Implementation Controls:** NIST SP 800-53: [Planning \(PL\)](#); [Program Management \(PM\)](#); and [SIMM 5305-A](#)