

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

**RISK ASSESSMENT**  
(Revised 12/13)

5305.7

**Policy:** Each state entity shall conduct an assessment of risk, including the likelihood and magnitude of harm from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system/asset and the information it processes, stores, or transmits. Each state entity shall conduct a comprehensive risk assessment once every two years which assesses the state entity's risk management strategy for all three levels and documents the risk assessment results in a risk assessment report.

The risk assessment process must include the following:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.
2. Identification of the state entity information assets that are at risk, with particular emphasis on the applications of information technology that are critical to state entity program operations. Identification of the threats to which the information assets could be exposed.
3. Assessment of the vulnerabilities, e.g., the points where information assets lack sufficient protection from identified threats.
4. Determination of the probable loss or consequences, based upon quantitative and qualitative evaluation, of a realized threat for each vulnerability and estimation of the likelihood of such occurrence.
5. Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level.
6. Selection of cost-effective security management measures to be implemented.
7. Preparation of a report, to be submitted to the state entity head and to be kept on file within the state entity, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of residual risk to be accepted by the state entity.

**Implementation Controls:** NIST SP 800-53: [Risk Assessment \(RA\)](#)