

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

**RISK ANALYSIS**  
(Revised 10/09)

**5305.1**

As an essential aspect of its information technology security and risk management program, each agency that employs information technology must establish a risk analysis process to identify and assess risks associated with its information assets and define a cost-effective approach to managing such risks. Specific risks that must be addressed include, but are not limited to, those associated with accidental and deliberate acts on the part of agency employees and outsiders; fire, flooding, and electric disturbances; and, loss of data communications capabilities.

The agency risk analysis process must identify and prioritize critical applications of information technology. When establishing priorities, agencies should consider that applications may become more critical as the period of unavailability increases and that processing cycles (i.e. monthly, quarterly or yearly) may have an impact upon the prioritization of applications. Agency risk management practices and disaster recovery planning must give priority to the establishment of policies and procedures to ensure the continued operation of these applications. See SAM Sections 5310 and 5355.

The risk analysis process must be carried out with sufficient regularity to ensure that the agency's approach to risk management is a realistic response to the current risks associated with its information assets. In general, the risk analysis process should be a cyclical process for most agencies. Agencies should complete the comprehensive risk analysis cycle at least every two years and whenever there has been a significant change in their use of information technology. This cycle ends with the preparation of a report documenting the risk assessment.

The risk analysis process should include the following:

1. Assignment of responsibilities for risk assessment, including appropriate participation of executive, technical, and program management.
2. Identification of the agency information assets that are at risk, with particular emphasis on the applications of information technology that are critical to agency program operations. A critical application, from a statewide perspective, is an application that is so important to the state that the loss or unavailability of the application is unacceptable. With a critical application, even short-term unavailability of the information provided by the application would have a significant negative impact on the health and safety of the public or state workers; on the fiscal or legal integrity of state operations; or, on the continuation of essential agency programs.
3. Identification of the threats to which the information assets could be exposed.
4. Assessment of the vulnerabilities, i.e., the points where information assets lack sufficient protection from identified threats.
5. 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.
6. Identification and estimation of the cost of protective measures which would eliminate or reduce the vulnerabilities to an acceptable level.
7. Selection of cost-effective security management measures to be implemented.
8. Preparation of a report, to be submitted to the agency director and to be kept on file within the agency, documenting the risk assessment, the proposed security management measures, the resources necessary for security management, and the amount of remaining risk to be accepted by the agency.