

Every organization has a mission. In this digital era, as organizations use automated information technology (IT) systems to process their information for better support of their missions, risk management plays a critical role in protecting an organization's information assets, and therefore its mission, from IT-related risk.

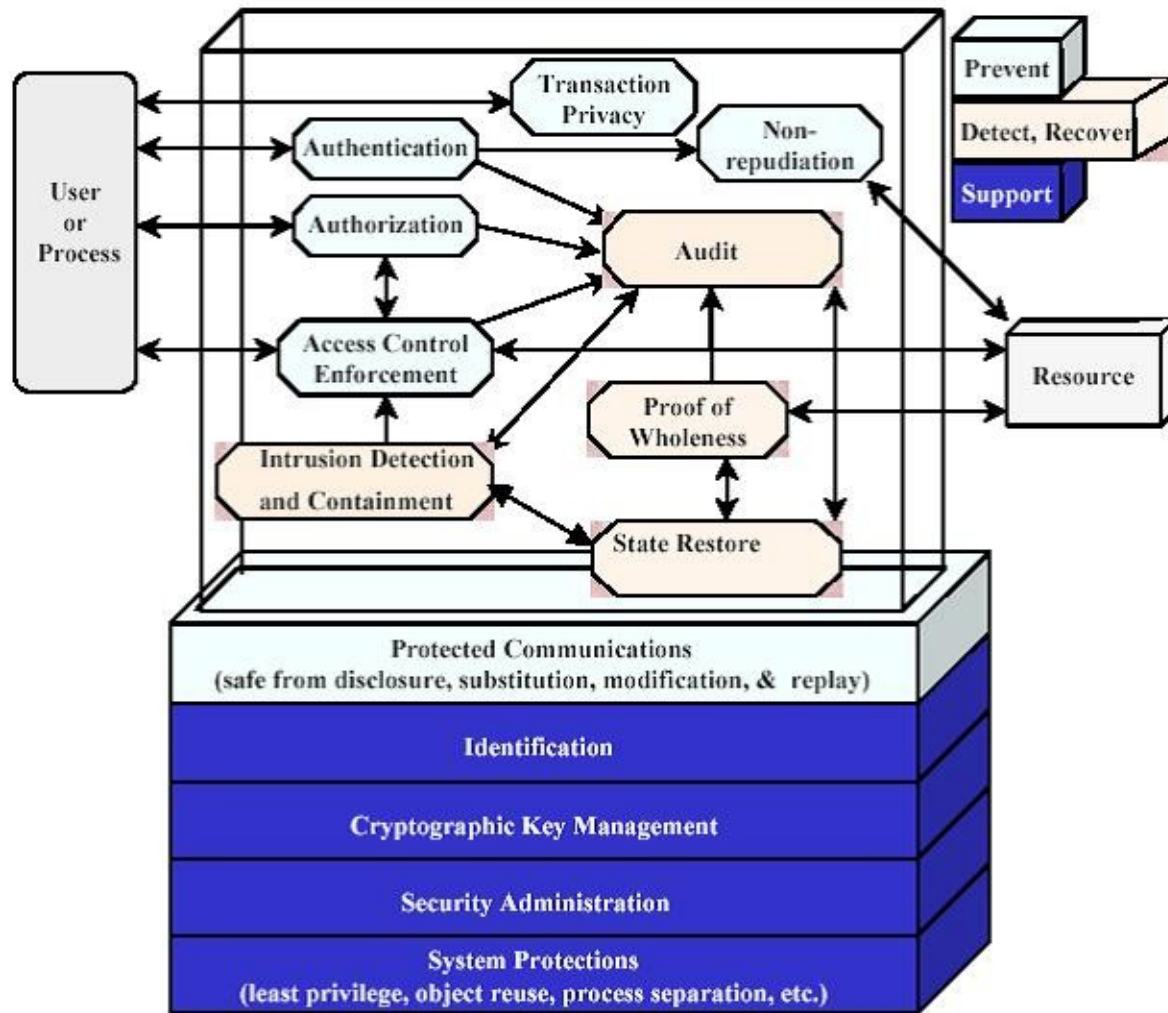
The National Institute of Standards and Technology's (NIST) Risk Management Guide, published in 2002, was written to provide organizations and professionals with a foundation to developing a successful and effective risk management program. The principal goal of an organization's risk management process is to protect the organization and its ability to perform their mission, not just its IT assets.

Risk management is the process of identifying risk, assessing risk, and then taking the appropriate steps to reduce risks to the organizations acceptable level. It encompasses three processes: risk assessment, risk mitigation and risk evaluation. The overall system security review considers both effectiveness and efficiency, including impact on the mission and constraints due to policy, regulation and laws.

Senior management plays a vital role in the risk management process. They hold the ultimate responsibility for mission accomplishment, and hence, must ensure that the necessary resources are effectively applied to develop the capabilities needed to accomplish the mission. They must also assess and incorporate results of the risk assessment activity into the decision making process. An effective risk management program that assesses and mitigates IT-related mission risks is not possible without the support and involvement of senior management.

The NIST Risk Management Guide defines a threat as the potential for a threat-source to exercise a specific vulnerability. Vulnerability is a weakness that can be accidentally or intentionally exploited. When there is no vulnerability, a threat-source does not present a risk. The responsibility for IT Security lies jointly in the hands of management, by issuing a budget for IT risk management, and technical personnel, by implementing appropriate risk management procedures. During the risk management process, if a potential vulnerability is identified, then security controls may be implemented to eliminate or reduce the magnitude of harm. Security controls can be of two kinds - technical and non-technical. Technical controls are safeguards that are incorporated into computer hardware, software or firmware. Nontechnical controls are management and operational controls.

Technical controls can be categorized into three major categories - support, prevent and detect and recover. The main support technical controls are - identification, cryptographic key management, security administration and system protection. The main preventive technical controls are - authentication, authorization, access control enforcement, nonrepudiation, protected communications and transaction privacy. The main recovery technical controls are - audit, intrusion detection and containment, proof of wholeness, restore secure state and virus detection and eradication. Management security controls, in conjunction with technical and operational controls, are implemented to manage and reduce the risk of loss and to protect an organization's mission. Management controls focus on the stipulation of information protection policy, guidelines, and standards which are carried out through operational procedures to fulfill the organization's goals and missions. The main control categories are represented in the figure below.



Source: NIST SP 800-30

Management security controls are comprised of three functions - prevention, detection and recovery. Preventive management controls are comprised of the following four operations:

- Assigning security responsibility to ensure that adequate security is provided for the missioncritical IT systems
- Developing and maintaining system security plans to document current controls and address planned controls for IT systems in support of the organization's missions
- Implementing personnel security controls, including separation of duties, least privilege, and user computer access registration and termination
- Conducting security awareness and technical training to ensure that end users and system users are aware of the rules of behavior and their responsibilities in protecting the organization's mission

Detective management controls are comprised of the following five operations:

- Implementing personnel security controls, including personnel clearance, background investigations and rotation of duties.
- Conducting periodic review of security controls to ensure that the controls are effective
- Performing periodic system audits
- Conducting ongoing risk management to assess and mitigate risk
- Authorizing IT systems to address and accept residual risk

Recovery management controls are comprised of the following two operations:

- Providing continuity of support and developing, testing and maintaining the continuity of operations plan to provide for business resumption and ensuring continuity of operations during emergencies or disasters
- Establishing an incident response capability to prepare for, recognize, report and respond to the

incident and return the IT system to operational status.

Operational security controls establish a set of controls and guidelines designed to ensure that security procedures governing the use of the organization's IT assets and resources are properly enforced and implemented in accordance with the organization's goals and missions. Management plays a vital role in overseeing policy implementation and in ensuring the establishment of appropriate operational controls. According to the Risk Management Guide, organizations after identifying all possible controls and evaluating their feasibility and effectiveness, should conduct a cost-benefit analysis for each proposed control to determine which tools are required and appropriate for their circumstances. The risk remaining after the implementation of new or enhanced controls is the residual risk. Practically no IT system is risk free, and not all implemented controls can eliminate the risk they are intended to address or reduce the risk level to zero.