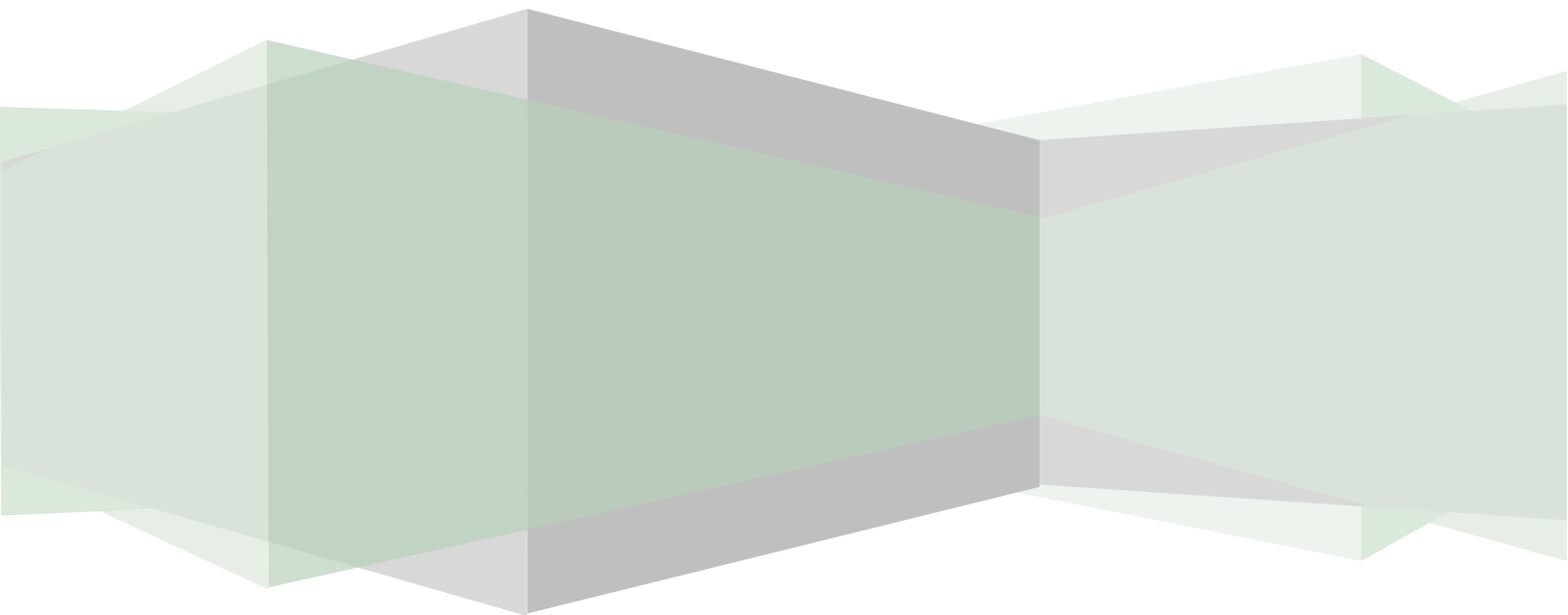




LORICCA
RELIABLE TECHNOLOGY SOLUTIONS

Managing Information Security

The Security Committee



Managing Information Security: The Security Committee

As a practical matter, large organizations should use a Security Committee to coordinate and manage their information security programs. The purpose of the Security Committee is to establish, manage, and maintain an information security program that:

- *Applies a coordinated and uniform approach to information security across all organizational units.*
- *Identifies and mitigates risk to data and business operations.*
- *Is auditable.*
- *If applicable, must be compliant with regulatory requirements.*

A Security Committee develops strategies that focus on protecting the enterprise. The Security Committee performs the following functions:

Risk Management Functions

- Manage risk via risk management and risk analyses processes.
- Establish an audit standard and process to proactively review and evaluate implemented security policy and technical measures
- Implement corrective actions, any required sanctions, and responses to address any security incidents.
- Periodically verify the recovery strategy and process for a catastrophic loss of information systems resources.
- Develop strategic security plans to enable the information security program to keep pace with the organization's goals and strategies.

Policy Management Functions

- Maintain formal security policies and procedures for management, the workforce, and outside parties that have access to the organization's information and information systems
- Establish and periodically review information security roles and responsibilities
- Review draft policies and policy revisions.

- Finalize, approve and distribute new policy and revisions.
- Provide for and verify the communication of security policies and procedures to the workforce, including establishing and maintaining ongoing training programs.

Technical Security Functions

- Coordinate IT implementation projects with required security projects.
- Monitor ongoing technical security product evaluation, design and implementation projects.
- Verify that the hardware, communications facilities, and software are adequately protected from performance or failures that could affect availability or security the organization's systems and information assets.
- Monitor and track the ability of communications facilities, network infrastructure, hardware and software to support security, availability and performance requirements.

Reporting Functions

- Report on significant risk management issues to Senior Management
- Periodically report to the Board or Senior Management on the Security Management Program
- Prepare reports on security incidents, the organization's responses, and final disposition.

Composition of The Security Committee

Any comprehensive information security program will affect both operations and a wide range of internal functions. The Security Committee should incorporate members who will be able to provide the committee with the widest possible view of the impact of identified risks, proposed polices & procedures, and technical safeguards. Members should include:

- ***Security Committee Chairperson*** - The Chairperson of the Security Committee should be a direct report to the CEO or Board. The actual position should be a staff function to allow for independence of the committee. Independence is crucial to ensure that management will be appropriately informed of security lapses and vulnerabilities that have significant risk to the overall organization.
- ***Administrative Advisor*** - The Administrative Advisor to the Security Committee will represent the administrative functions of the organization.

- **Operations Advisor** - The Operations Advisor will be responsible for representing the various enterprise-wide operational departments.
- **Technical Advisor** - The Technical Advisor will advise the committee on the technical issues associated with the Security Committee. The Technical Advisor will also be responsible for verifying the reliability, availability, and maintenance of the computer infrastructure that supports the administrative functions and operations.
- **Management Advisor** – The organization may choose to include a Management Advisor on the committee to ensure that the committee considers strategic as well as tactical issues in managing the security program.

Security Committee Subcommittees

Subcommittees are an efficient method of distributing the workload and assigning specific tasks to those with expertise in affected areas. Subcommittees should regularly report progress to the Security Committee. Subcommittees of the Security Committee can include members that are not on the Security Committee. Some examples of this include the:

- **Administrative Policy and Procedure Subcommittee** - The Policy and Procedure Subcommittee will approve the specific procedures that are implemented to adhere to the policies that have been adopted. Appropriate representatives from each administrative department should serve on this subcommittee. The Administrative Advisor will chair this subcommittee.
- **Operations Standards Subcommittee** - The Operations Standards Subcommittee will establish appropriate information and operational standards to enable the organization to conduct its business. The Operations Standards Subcommittee should include representatives from key mission-critical operational departments. The Operations Advisor will chair this subcommittee.
- **Regulatory Monitoring Subcommittee** – If needed, The Regulatory Monitoring Subcommittee should be responsible for monitoring the regulatory (state, federal, etc.) compliance issues that may affect the security management program.
- **Technology Subcommittee** - The Technology Subcommittee will monitor the status of information technologies in light of security and performance requirements, as well as adherence to the adopted information technology security policies and procedures, which should be designed to ensure the availability, integrity and confidentiality of business critical data. The Technical Advisor will chair this subcommittee.

- **Authorization Subcommittee** - The Authorization Subcommittee will authorize the extension of access to corporate information, usually on a need-to-know basis, such as RBAC (role based access control). The Authorization Subcommittee will verify the extension of data access to individual employees and contractors, as well as authorize unilateral or bi-lateral electronic business relationships with any outside parties. The Security Committee Chairperson will chair this subcommittee.

The protection of your organization and its assets from a realized security threat, due to either a known or unknown vulnerability, requires a comprehensive approach that marshals the information systems, administrative, operational, and management resources of your entire organization. Only when there is involvement from each of these business areas, coupled with workforce training on the adopted security policies and procedures, can an organization reduce its vulnerability to security threats, and move forward with an effective Risk Management Program.

Michael Whitcomb, PMP, CISM

Michael is the founder and President of **Loricca, Inc.** He has 25 years of experience building and supporting secure systems for government and commercial organizations of all sizes. Michael brings the technical knowledge and proven leadership ability for Loricca to provide world class security services. Since founding Loricca, Michael has established the company's presence providing security solutions to some of the country's largest companies.

Prior to Loricca, Michael served in technical leadership positions, leading and implementing solutions for various clients within both the government and commercial sectors including finance, healthcare, retail and federal government. Michael holds a Bachelor of Science in Management of Information Systems from the University of Phoenix in addition to the PMP and CISM professional certifications.

Loricca, Inc. | www.loricca.com | 813.600.3005 | mwhitcomb@loricca.com