The Technology Trilogy:

Security, Disaster Recovery, & Business Continuity

Information Technology Services for Colleges and Universities

www.ThinkEduServe.com

The Technology Trilogy:
Security, Disaster Recovery & Business Continuity

One of the hottest topics today – regardless of the source—is the protection of information. Newspapers, popular magazines, broadcast television, blogs, and government reports are discussing how information technology can and has been compromised, and ways to avoid being the victim of an attack. Colleges and universities are particularly vulnerable because of the sensitive nature of the information stored and processed– social security numbers, credit card information, financial information, addresses, personal schedules and transcripts are particularly enticing to identity theft criminals.

In addition to unwanted and uninvited intrusion, colleges and university must also be aware of their vulnerabilities to natural disasters, and to threats toward people, systems and buildings. Tornadoes, hurricanes, and earthquakes can wreak havoc on the continuity of university business operations. And, many institutions fail to plan in the event critical staff members are unable to perform their duties.

State legislatures, boards of trustees and Presidents are now requiring comprehensive disaster recovery plans. In most cases, the disaster recovery plan provides for an alternate computing environment should there be a fire or flood, and identifies backup procedures. Often, this is focused entirely on the technology environment, and neglects to fully address business continuity in the event of a disaster.

We believe that taking a holistic approach to Security, Disaster Recovery and Business Continuity provides the framework for maximum protection and will significantly reduce downtime in the event of a disaster. Our model aligns these three most vulnerable points (security, disaster recovery, and business continuity), and connects all three to create an environment that is:

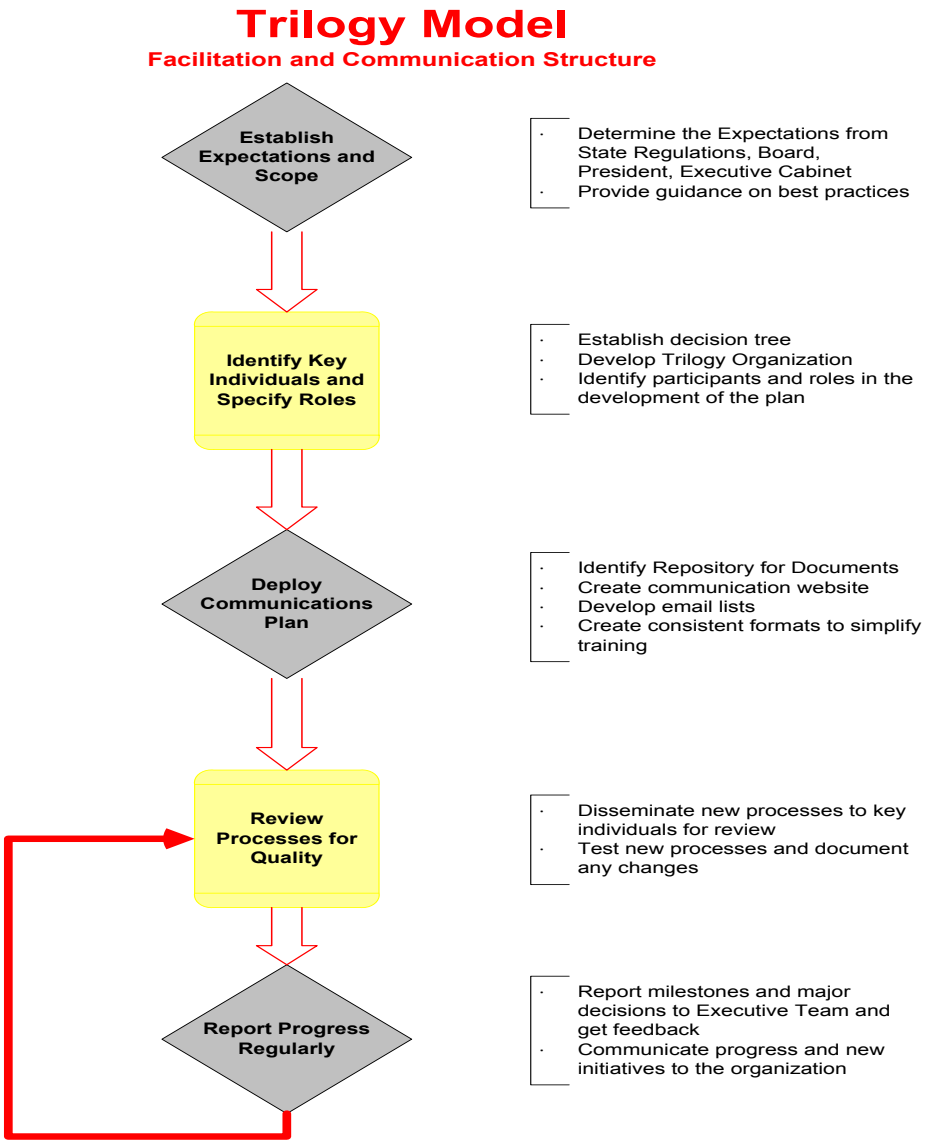
- Resistant to attack
- Able to quickly and efficiently recover from any disruption
- Able to continue to perform business operations within institutional expectations

The *Trilogy Model* was developed to strengthen each planning process, identify and address all vulnerabilities proactively, and reduce the time and effort required to develop separate plans. And, because the model integrates a wider range of users it also helps to reinforce the individuals' role in security, disaster recovery and business continuity.

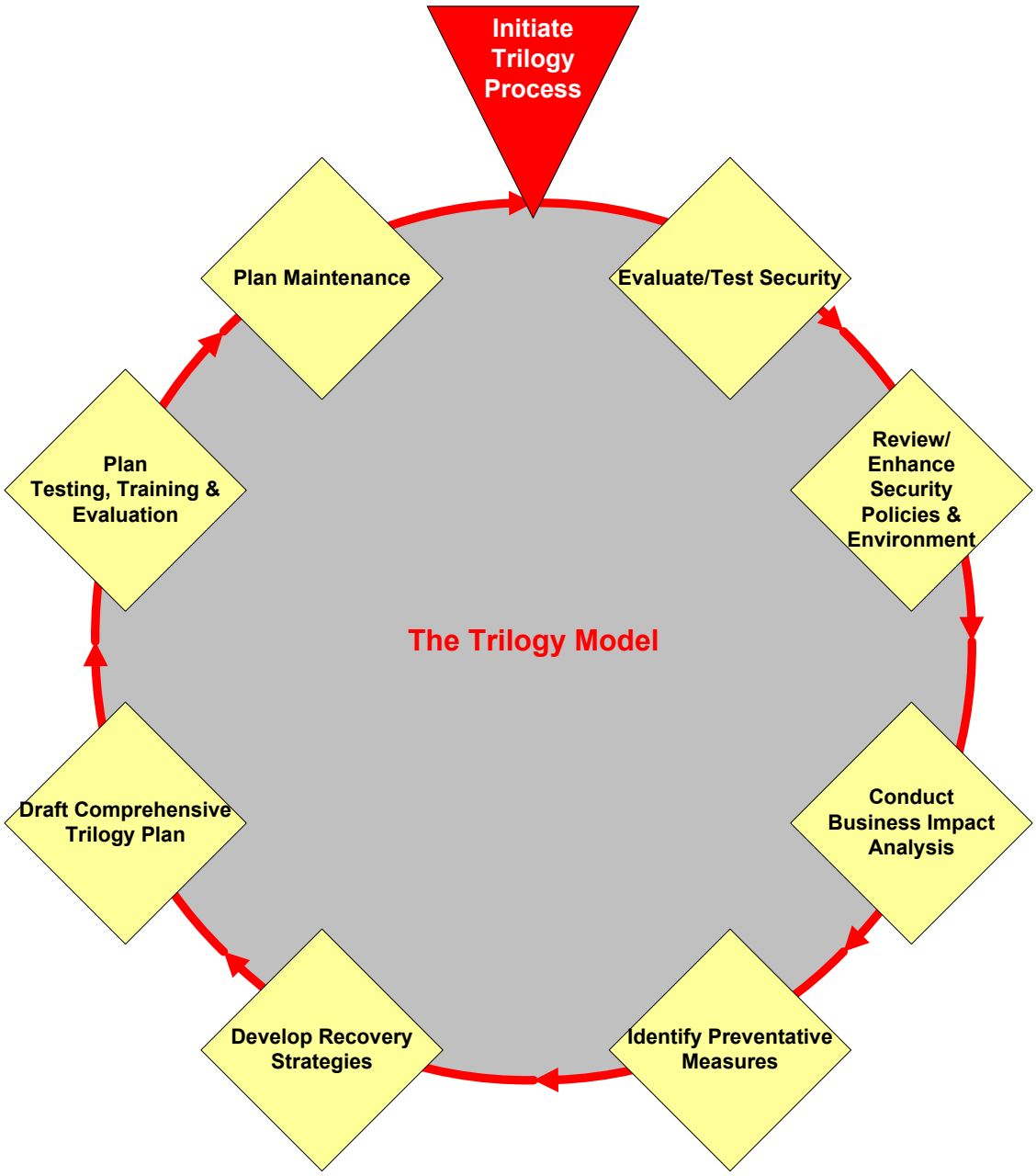
The Trilogy Model: Planning Process & Standards

The *National Institute of Standards and Technology* developed a set of guidelines for Disaster Recovery and Business Continuity Plans. The Trilogy Model utilizes the *NIST* guidelines to ensure that all plans meet state and federal regulations.

The Trilogy Model provides a comprehensive approach to data collection as well as an organization for including the appropriate people within the organization. The communication and facilitation structure is critical for the success of the plan development. Elements of quality assurance and practical change management are interwoven throughout the structure.



The facilitation and communication structure provide the guidelines for deploying the actual Security, Disaster Recovery and Business Continuity process. This process is managed by a project manager who is able to guide the institution through each step of the model. The Trilogy Process is illustrated below:



In essence, the process includes:

- Assessment of the current security environment and direction for strengthening and hardening the infrastructure and policies.
- Contingency Policy & Organization – The organization establishes a policy that provides the authority and guidance to develop a plan. In addition, it establishes an appropriate organizational structure to react and participate in contingency planning as well as disaster recovery.
- Business Impact Analysis – Every organization must identify its critical systems and components to ensure business continuity. It must determine what the impact of system loss may be and determine recovery priorities.
- Identify Preventative Measures – Through the analysis, potential hazards will be identified and recommendations for remediation and prevention will be listed.
- Develop Recovery Strategies – Working with the staff and administration, a series of recovery strategies will be developed. In addition to the strategies, costs and resources will be identified.
- Create the Contingency Plan – From the data gathered from the first four steps in the series, the actual Contingency Plan document can be written. This document will provide the institution with specific procedures for recovery as well as all other pertinent information such as personnel contact information, memoranda of understanding, etc.
- Test, Train and Evaluate – Testing enables the plan deficiencies to be identified and addresses as well as evaluate the ability of the recovery staff to implement the plan effectively. Periodic, systematic training for all recovery personnel is essential as well.
- Plan Maintenance – In order to ensure that the plan remains viable it must be updated periodically. This should part of an overall strategy, and testing and revision should occur regularly.

Sample Table of Contents

Below is a sample Table of Contents for a comprehensive Trilogy Plan:

Development of comprehensive contingency plans requires extraordinary expertise. Such expertise includes:

- Tactical Planning
- Knowledge of Contingency Planning Standards
- Organizational Leadership and Group Facilitation Skills
- Information Technology & Systems Design
- Network and Infrastructure Design

- Business Process Analysis
- Technical Writing
- Presentation Skills

In addition, developing a contingency plan requires many dedicated hours to collect information, document processes, develop strategies and create an effective planning document.

Many institutions have found it not only cost effective, but far more efficient to utilize the services of a contingency planning consultant to facilitate the process.

Conclusion

EduServe is a management consulting firm specializing in higher education. EduServe is dedicated to helping colleges and universities accomplish their mission through maximizing human performance and realizing technology's potential. **Our mission is to produce extraordinary results for the colleges and universities we serve.** Higher education management is our core business; as expert practitioners, EduServe consultants have an average of 20 years each serving higher education. EduServe understands the challenges you face. We guide you in the use of best practices and in adopting emerging methods for effective institutional and technology management.

Our unique blend of leadership, management and planning expertise allows us to work creatively with our clients to build workable strategies and deliver measurable results.

For more information on EduServe's Contingency Planning services and deliverables, please contact us: