

Session T2 – Security Best Practice and Compliance: What You Need to Know to Bridge the Gap and Meet Network Auditing Requirement

Topic Summary

With the growing volume of regulatory standards, organizations need to design and implement systems to unify all regulatory compliance initiatives under one umbrella security policy to meet due care and audit requirements. Successful companies will develop a comprehensive internal security policy to defend their regulatory compliance and then implement systems to ensure that those standards are consistently being met across the organization – and help ensure their audits are a success.

Learning objectives for the session include:

- How to comply with multiple regulatory mandates such as SOX, GLBA, HIPAA and FISMA – and increase audit coverage and frequency.
- Understanding the role of auditing frameworks such as ISO 17799, CobiT
- Why it's more important than ever for organizations to implement and maintain a strong security policy.
- What to consider when implementing security policies to meet audit requirements.

A cross section of departments are tasked with influencing security and regulatory compliance initiatives within an organizations, including senior management, finance departments, audit groups and security and IT departments.

This four session program will cover materials relevant to all of these audiences with the goal of establishing a framework for these groups to collaborate and meet critical network audits. Particular emphasis will be placed on topics affecting the security groups typically responsible for controlling regulatory compliance process development and implementation.