Risk Management: *Security Governance for Business Optimization*

SESSION #28

Panel discussion with IT executives to share strategies and techniques for establishing effective information security governance.

Security Environment Overview

- POLICIES AND REGULATIONS
- TERMS AND DEFINITIONS

State Administrative Manual (SAM)

- **Chapter 5300, *Information Security*, Section 5305**

- State entities are responsible for establishing an information security program to manage risk, protect their information assets and prevent illegal activity.
- Includes establishing a **governance body** "to direct the development of state entity specific information security plans, policies, standards and other authoritative documents".

Statewide Information Management Manual (SIMM)

- **SIMM 5305-A *Information Security Program Management Standard***

- "Leadership, organizational structure, communications, relationships and processes form the basis of information security governance."
- A Governance Framework refers to a "top-down executive management approach to establish, implement and govern the information security program."

Federal and State Regulations

- Federal Information Processing Standards (FIPS). FIPS 199 deals with information system security categorization. FIPS 200 specifies minimum security requirements for federal information systems.
- The National Institute of Standards and Technology (NIST), Special Publications. NIST 800-53, 800-30 and 800-39 deal with security and privacy controls and risk management.
- State regulations related to information security include:
  - Government Code 11545-6 – CDT and state entity roles/responsibilities
  - GC 11549 – CISO functions
  - Civil Code 1798 – Information Practices Act, updates include addressing data breaches, criteria for meeting definition of "personal information"

PANEL MEMBERS

- RAYFIELD SCOTT
- KEITH TRESH
- CHRISTINE SCHMOECKEL

QUESTIONS FOR THE PANEL

QUESTIONS FOR PANEL

- How did your organization go about establishing information security governance program, beyond the basics of designating an ISO. What role did you play in setting up the program and how do you participate or otherwise interact with it now?

QUESTIONS FOR PANEL

- What challenges have you faced in ensuring information security was given the appropriate priority in your organization? How have you overcome these challenges?

QUESTIONS FOR PANEL

- What, if any, interfaces does security at your organization have with configuration/change management processes with respect to day to day operations and/or IT projects?

QUESTIONS FOR PANEL

- How have you been able to participate in business decision making (as opposed to strictly IT related decision making) in your organization as it relates to addressing information security?

QUESTIONS FOR PANEL

- Are there any specific tips, strategies or techniques you can share that might help others in a similar position to implement effective information security governance?

QUESTIONS FROM THE AUDIENCE ??????