

**Commonwealth Information Security Council
Risk Management Committee Meeting
May 18, 2009
2:00-3:00
CESC (Madison)**

Risk Management Committee members attending:

Rob Jenkins, DJJ, Co-Chair
Goran Gustavsson, APA, Co-Chair
Jack Spooner, DOA
Ross McDonald, DSS
Jeremy Greenwood, TRS
Joshua Cole, Dept of Aviation

Risk Management Committee members absent:

Aaron Mathes, OAG, Co-Chair
Bob Auton, DJJ

Also Attending:

Peggy Ward, VITA
Mauri Shaw, VITA

Topic: Risk Management Requirements

- **Requirements - Discussion**
- Ross McDonald prepared and the committee discussed:
 - Risk Management requirements from COBIT 4.0, SEC501-01, v4,
 - The background/Basis of SEC501-01, v4, NIST 800-53, FISCAM, ISO 27002
 - Potential training strategies, an overview Risk Management topics and resources for various roles within agency information systems environment ("IT Risk Management – Examples of Training Modules")
- Goran Gustavsson prepared and the committee discussed an overview of 50 agencies tested for adequate implementation – (The remaining 24 agencies did not have an adequate program and were not tested for implementation).
- Follow-up in 2 weeks in Richmond – meeting at DJJ – June 1, 1:30 p.m.
 - Information Gathering – Responsibilities from SEC501 – Gap review of training module to SEC501, 506.

Topic: Risk Management Goals and Objectives

- Rob Jenkins prepared and the committee has approved the following Risk Management Committee – Goals and Objectives:

Risk Management Committee -Goals and Objectives

- Increase Awareness of the Importance of Risk Management to Commonwealth Governmental Organizations
 - High Level Presentations to Educate - How does Risk Management fit within the larger context of Information Security - use IT Security Framework as a roadmap (?)
 - ISOAG Meeting
 - AITR Meeting
- Education
 - More in depth training similar to ISO Orientation
 - Research IREC for applicable material
- Support
 - ISOAG Portal for material and discussion
 - Identify Subject Matter Experts to monitor discussion
 - Templates - SharePoint as a repository
- Analysis
 - How the change in standards impacts costs/benefit"
 - How to use Risk Analysis tools as part of the decision process