

**Commonwealth Information Security Council
Risk Management Committee Meeting**

June 1, 2009

1:30-3:00 pm

DJJ (700 East Franklin Street)

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
Bob Auton, DJJ

Risk Management Committee members absent:

Aaron Mathes, OAG, Co-Chair

Also Attending:

Mauri Shaw, VITA

Topic: Risk Management Training Considerations

1. Overview – Use NIST 853/NIST SP830 or SEC 501
2. Types of Risk Management
 - a. Project Risk Management
 - b. Operational Risk Management
 - c. Financial Risk Management
 - d. Technical Risks (upgrades, etc.)
 - e. Service Based Risk – the risk to a service of which IT might only be a part of the service, Service Orientated Architecture.
3. Linking Risk Management (IT & Executive/Operational Management)
 - a. How do you use within an organization
 - b. Formal vs. informal
4. Communications – Use ARMICS documentation
5. Common Glossary/Data Dictionary
 - a. 506 and 501 has terms and rating systems