



CESC, Madison Conference Room December 13, 2012 – 1:00 – 2:30

Members Attending Meeting:

Bob Auton (DJJ)
Bob Haugh (VDEM)
Goran Gustafson (APA)
Richard Benke (WWRC) *
Dennis Casey (VMNH) *
Melanie Seigler (DOF) *

CSRM Support:
Bill Freda (VITA)

* Attending Via Teleconference

Next Meeting:

CESC, Washington Conference Room
January 28, 2013 – 1:00 – 3:00

Opening ISO Manual Meeting

Topics included:

- Discussion of purpose and content of the manual.
 - Potential topics to include
 - Procedures for the Security Exception Process
 - Security Folder
 - Group Management
 - Clear direction of requirements
 - Agency responsibilities matrix
 - ISO duties: compliance and business related
 - Table of Contents
 - Post Meeting submission (included)

ISO Manual

Proposed Table of Contents

- 1) So You've Just Been Appointed as Your Agency's Information Security Officer (10 Things You Should Do Immediately)
- 2) The Commonwealth's Information Security Governance Structure
- 3) Everything You Wanted to Know About SEC 501 But Was Too Afraid To Ask
- 4) The Agency's Information Security Program (The View From 50,000 Feet)
- 5) The Supporting Cast
 - a. Who (or what) is a System Owner and What Do They Do
 - b. Who (or what) is a Data Owner and What Do They Do
 - c. What Is the Role of the Commonwealth Information Security Office
- 6) Business Process Analysis (Or Finding Out What Your Agency Really Does)
- 7) Sensitivity Analysis (Without the Help of a Shrink)
- 8) Risk(y) Assessment (Business)
- 9) Information Security Training
- 10) Agency Level Security Policy (The ISO's Opportunity to be King/Queen for a Day)
- 11) Responding to Security Incidents
- 12) Disaster Recovery ≠ Continuity of Operations
- 13) Exceptions, Exceptions, Exceptions
- 14) Audits Can Be Your Friends

Following is a list of suggested appendices:

- 1) ISO Flow Chart
- 2) Documentation List
- 3) ISO Calendar