40.2 Information Security Continuous Monitoring

ISCM

> Maintaining ongoing awareness of Information Security, vulnerabilities, and threads to support organizational risk management solutions.

ISCM Process

- *Define:* Determine objectives and desired outcome of the program
- *Establish:* What information do we want to collect?
- *Implement:* Collect appropriate data we need to make our decisions
- *Analyze/Report:* Right resources to analyze those reports
- *Response:* To any anomaly based on the reports results
- *Review/Update:* Re-iterate process, and flatten out problems

Establish a ISCM Program

Requires the organization to define criteria and processes including:

- Metrics
  - Derived from specific objectives
- Frequency of data collection
  - Collection, assessment and monitoring based on events such as:
    - Security control volatility
    - System categorization and classification
    - Security control with identified weaknesses
    - Organizational risk tolerance
    - Threat information
    - Vulneability information
- ISCM implementation tools and metrics
  - Automate every process available

SCAP - Security Content Automation Protocol

> Suite of specifications to enable automated vulnerability management, measurement, and policy compliance.