Data Analytics for Compliance

Compliance Is Hard

Brent White brent.white@ironbow.com
Iron Bow Technologies
Data Analytics Specialist

Agenda

Risk Management

Security attacks to Information Systems cannot be eliminated so they must be managed.

- Components of Risk Management
  - Identifying areas of risk in the Information System
  - Assessing risk
  - Responding to risk
  - Monitoring risk
- Identify threats, vulnerabilities, likelihood and impact

Examples of information systems include:

- Email systems
- Personnel systems
- Weapons systems
- Enterprise Resource Planning (ERP) tools
- Enterprise and local networks
- And many others

DIACAP vs RMF

DIACAP

The DoD Information Assurance Certification and Accreditation Process

Compliance does not equal Security

- Compliance has typically been a check box
- Not a security tool
- Does not improve security posture
- Not a real-time or near real time assessment of security posture

RMF Steps


NIST Risk Management Framework
Architectural Description
Architecture Reference Models
Segment and Solution
Architectures Mission and
Business Processes Information
System Boundaries
Process
Overview
Organizational Inputs
Laws, Directives, Policy Guidance
Strategic Goals and Objectives
Priorities and Resource Availability
Supply Chain Considerations
Starting Point
Repeat as necessary
Step 1
Categorize
Information
System
Step 2
Select
Security Controls
Step 3
Implement
Security Controls
Step 4
Access
Security Controls
Step 5
Authorize
Information
System
Step 6
Monitor
Security Controls
Risk
Management
Framework

RMF is a Six Step Model

Step 1 – Categorize the Information System (IS)

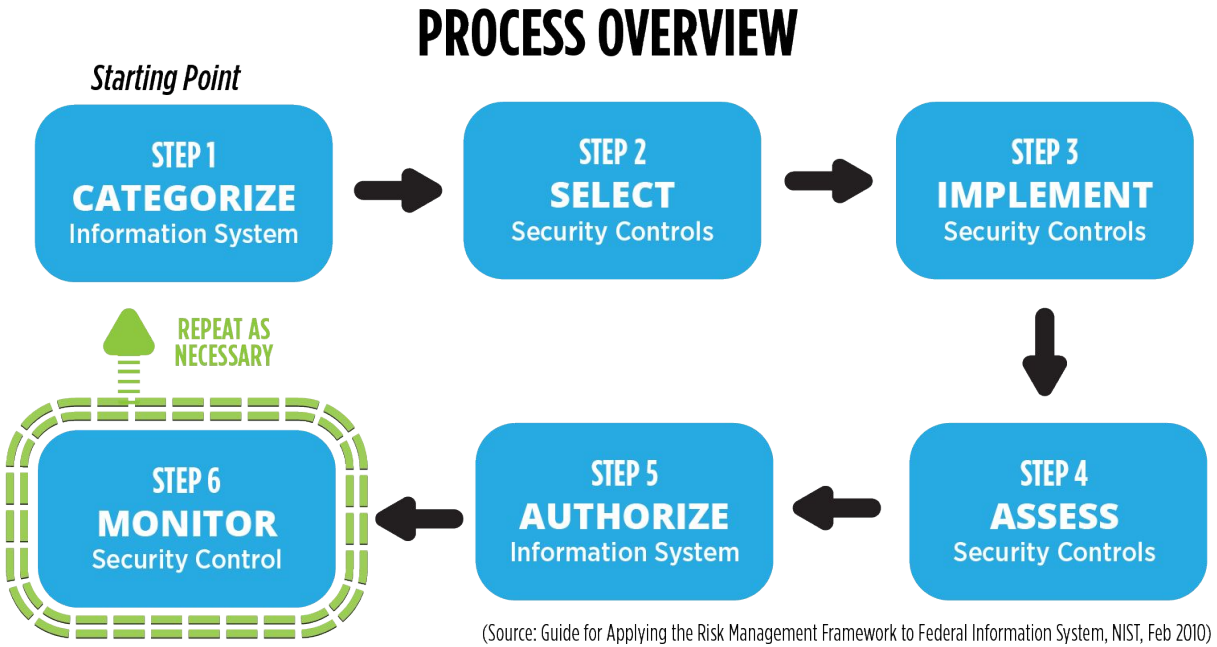
- Categorize the information processed, stored and transmitted
- Identify ALL potential risks, both electronic and physical, that would occur if the information is compromised
- Rank impact – High / Medium / Low

Step 2 – Select Security Controls

- Identify which of the 120+ controls identified by NIST should be implemented

Step 3 – Implement Security Controls

- Document how controls are deployed and used within the system
- Detail any corrective action if a security violation occurs



(Source: Guide for Applying the Risk Management Framework to Federal Information System, NIST, Feb 2010)

RMF is a Six Step Model

Step 4 – Assess Security Controls

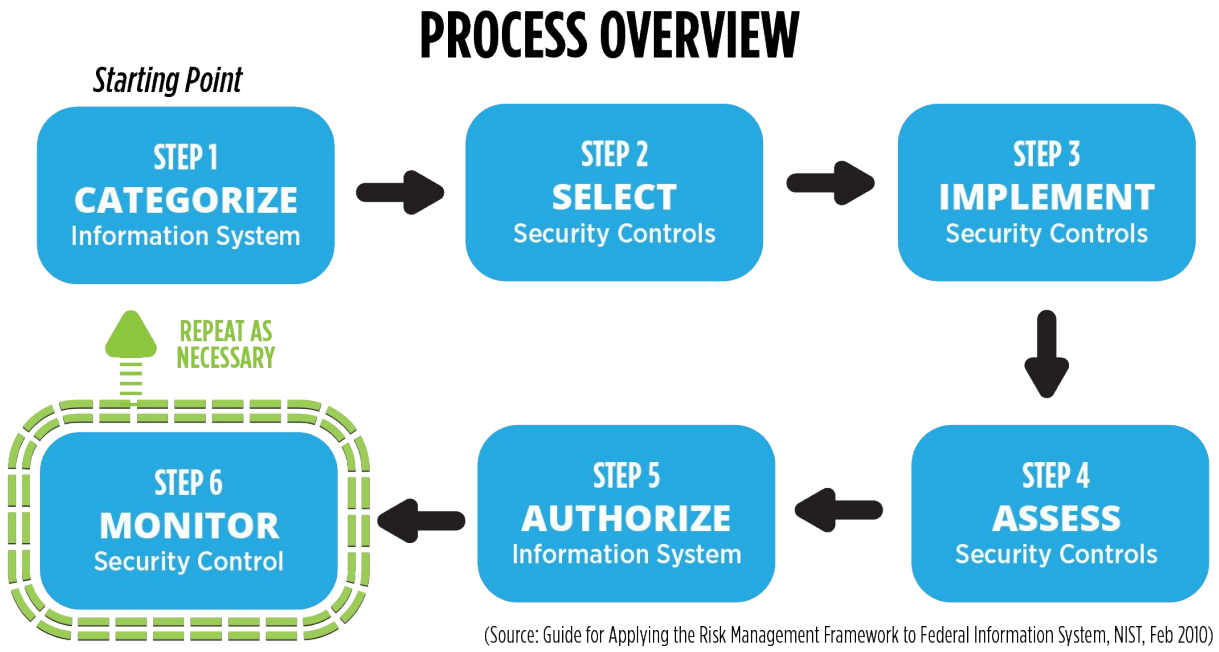
- Ensure controls implemented meet both security and mission for the system being accredited
- Continually monitor and maintain controls

Step 5 – Authorize the Information System

- Assess controls, determine if risks have been significantly mitigated
- If yes, the system will be authorized to process information
- An audit can be required anytime

Step 6 – Monitor the Information System

- Continuously monitor the controls and assess effectiveness
- Update documentation regularly



* March 12, 2014 DOD instruction # 8510.01

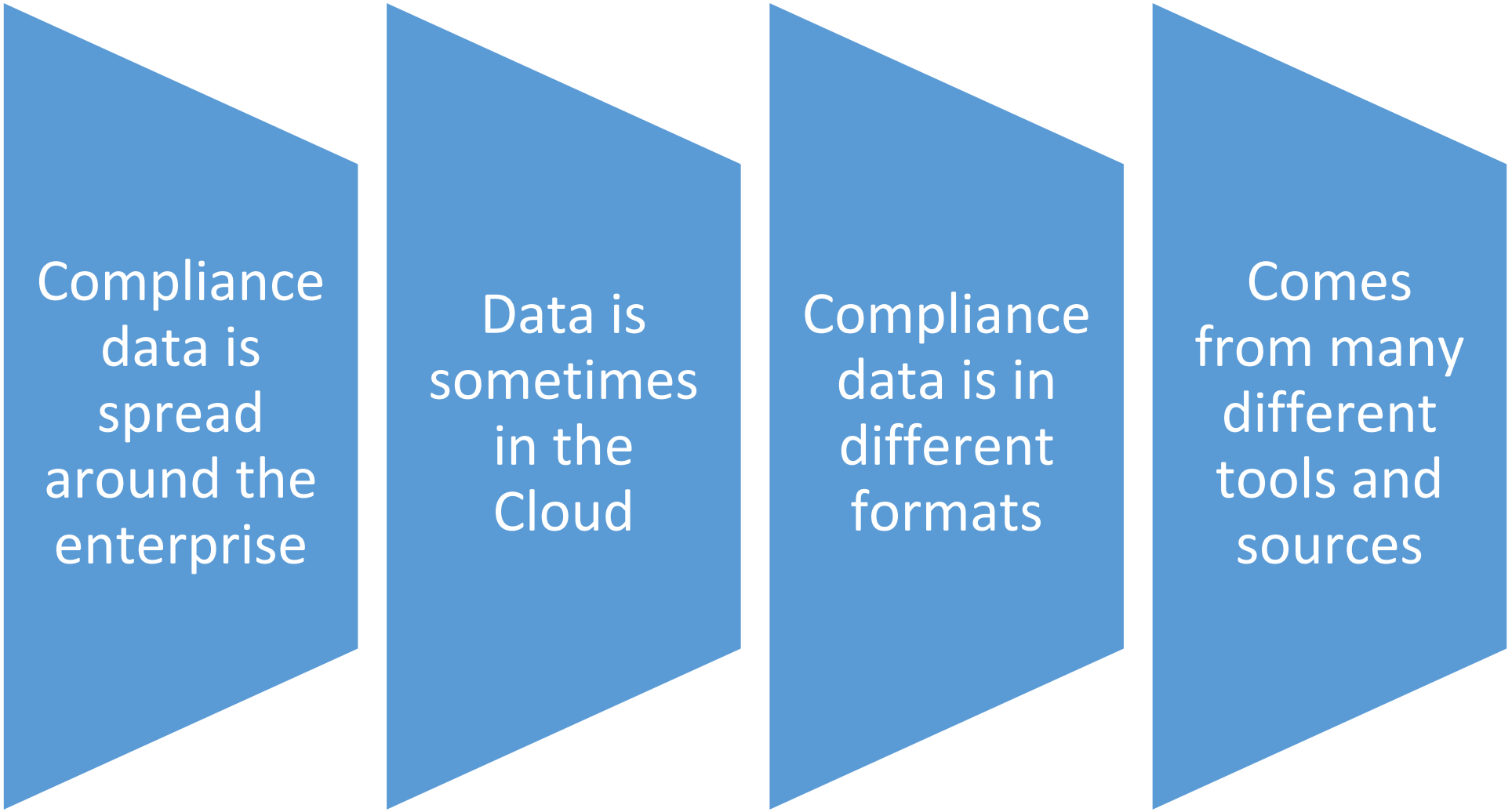
"continuous monitoring capabilities will be implemented to the greatest extent possible"

eMASS
Enterprise Mission Assurance Support Service

Compliance challenges

- Time Consuming
- Limited security value
- Exercise in Excel Spreadsheets
- Framework Updates
- Moving target

Where is my Compliance Data?



Simplify Compliance

Use big data analytics:

- Bring all compliance data into a single location
- Analyze all of that data for compliance reporting
- Continuous near real-time monitoring of compliance and security posture
- Use pre-built reports and dashboards designed specifically around NIST requirements

DEMONSTRATION

AUTOMATE MONITORING AND REPORTING!