Department wide Gap Analysis & Establishing a Tier 2 Information Security Risk Management Program

Debra Graul, Information System Security Manager
Taryne McDonald, Information Owner
Outline

- Rationale
- Fundamentals of Gap Analysis
  - Standards, Metrics, & Project Management
- Results
  - Findings & Recommendations
- Implementation
  - Current State & Future Plans
- Conclusion
Rationale

Risk Management Framework (NIST SP 800-37)

Tier 1: Enterprise Cybersecurity Department

Tier 3: Information System Level
7 distinct Security Boundaries

Directives, Standards, & Policies

Process, Procedures, & Guidelines

Standard Operating Procedures

Agency Dashboards & Reporting

Program Dashboards & Metrics

System Metrics & Reporting

Missing
Foundation for Gap Analysis
Gap Analysis: Standards

NIST

- NIST SP 800-30: Guide for Conducting Risk Assessments
- NIST SP 800-37: Risk Management Framework
- NIST SP 800-53: Security & Privacy Controls for Federal Information Systems & Organizations
- NIST IR 7358: Program Review of Information Security Management Assistance (PRISMA)

ISACA Risk IT Framework

- Governance, Risk Management & Compliance Framework
- Align the management of business risk with agency & department tolerances
- Balance costs & benefits of managing risk, based on business impact assessments
- Promote fair & open communication of risk between all stakeholders
- Establish a continuous process that is part of daily activities
Gap Analysis: Standards

Key Practice Areas (KPAs) identify core area of information systems security risk management for this analysis. The attributes serve as an indicator of the effectiveness of the systems for that practice area. KPAs and attributes provide context and consistent evaluation of the system’s security and risk management.

Key Practice Area 1 - Information Security Deliverables
1.1 Completeness
1.2 Quality/Accuracy

Key Practice Area 2 - Resources Core Competencies
2.1 Education, Training and Experience
2.2 Security Knowledge & Technical Expertise

Key Practice Area 3 - Processes, Procedures & Standard
3.1 Controls Review & Assessment
3.2 Adherence to Risk Management
### Gap Analysis: Metrics

**Metrics allow for:**

- Quantifiable measures for the KPAs using defined attributes
- Objective review of the Risk Management Standards
- Baselining current state of risk across all security boundaries
- Ability to set goals for a department wide risk management & continuous monitoring program

<table>
<thead>
<tr>
<th>Category</th>
<th>Description</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Emergent understanding that IT risk is important and needs to be managed.</td>
</tr>
<tr>
<td>Defined</td>
<td>IT risk management is viewed as a business issue, and both downside and upside of IT risk are recognized.</td>
</tr>
<tr>
<td>Managed</td>
<td>IT risk management is viewed as a business enabler, and both the downside and upside of IT risk are understood.</td>
</tr>
<tr>
<td>Optimized</td>
<td>Senior executives make a point of considering all aspects of IT risk in their decisions.</td>
</tr>
</tbody>
</table>
## Gap Analysis: Metrics

<table>
<thead>
<tr>
<th>Metric</th>
<th>KPA 1.1 – Completeness Attribute Measured Criteria</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>The risks are not identified in the deliverable. The controls are not mapped against the risk appropriately. Does not provide sufficient narrative in describing risk aspects of the system in relation to the deliverable’s objective. Does not provide sufficient supporting evidence for determinations of system related risks.</td>
</tr>
<tr>
<td>2</td>
<td>The risks are not completely identified in the deliverable. Most of the controls are mapped against the risk appropriately. Does not provide sufficient narrative in describing risk aspects of the system in relation to the deliverable’s objective. Does not provide sufficient supporting evidence for determinations of system related risks.</td>
</tr>
<tr>
<td>3</td>
<td>The risks are somewhat identified in the deliverable. The controls are mapped against the risk appropriately. Information Security deliverable provides some narrative in describing risk aspects of the system in relation to the deliverable’s objective. Does not provide sufficient supporting evidence for determinations of system related risks.</td>
</tr>
<tr>
<td>4</td>
<td>The risks are completely identified in the deliverable. The controls are mapped against the risk appropriately. Information Security deliverable provides sufficient narrative in describing risk aspects of the system in relation to the deliverable’s objective. Information Security deliverable provide sufficient supporting evidence for determinations of system related risks.</td>
</tr>
</tbody>
</table>

**KPA 1.1 – Completeness Attribute**

**Completeness of Information Security Deliverables** – It is always recommended the overall system narrative for any system be complete and consistent, ensure description of risk areas in the proper level of detail (boundary, data sensitivity, applied controls etc.).

To determine the completeness the entire set of deliverables are reviewed individually & comparatively against each other to:

- Ensure risks are consistently reviewed with supporting evidence and cited rationale for determination of risk
- The details are complete including comprehensive references to NIST controls and standards in the risk narrative
- Ensure that the system security documents are reviewed on an defined basis via continuous monitoring
Gap Analysis: Project Management

- Stakeholder Interviews
- Scope, Goal, Objectives
- Project Planning Document
- Communications Plan
- Project Schedule
- Project Charter
- Kick-off Meetings
- System & Program Assessment Results
Gap Analysis: Project Management

- Communications with ISO / IO / CORs was key early in project to ensure clarify scope, set expectations, & to gain buy-in of their support

- Early delivery of references to security team helped avoid surprises & allowed for sufficient responses on their part

Security Documentation List

<table>
<thead>
<tr>
<th>No.</th>
<th>Document/Title/Description</th>
<th>NIST Control</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>Information System Fail Assessment</td>
<td>EA-GA</td>
<td>Yes</td>
</tr>
<tr>
<td>2</td>
<td>Security Strategy Plan (SSTP) Checklist</td>
<td>CA, CA, (ISAST, GSA)</td>
<td>Yes</td>
</tr>
<tr>
<td>3</td>
<td>Privacy Technical Assessment [Report/Impact Assessment Final]</td>
<td>IC, IC</td>
<td>Yes</td>
</tr>
<tr>
<td>4</td>
<td>Security Document</td>
<td>CA, SI</td>
<td>Yes</td>
</tr>
<tr>
<td>5</td>
<td>ARP Documents</td>
<td>CA</td>
<td>Yes</td>
</tr>
<tr>
<td>6</td>
<td>All Risk Assessments (if not included in report)</td>
<td>Applicable</td>
<td>Yes</td>
</tr>
</tbody>
</table>

<table>
<thead>
<tr>
<th>No.</th>
<th>Document/Title/Description</th>
<th>NIST Control</th>
<th>Reference</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>Non-realization Understanding (Including Interagency Security Agreement (ISA) Revisions)</td>
<td>IC, IC, IC, IC, IC</td>
<td>Yes</td>
</tr>
<tr>
<td>8</td>
<td>Detailed System/Network Architecture Diagram with Addressing of Issues that will be leveraging [if not included in SSTP]</td>
<td>AD, AD, CM, MI</td>
<td>Yes</td>
</tr>
<tr>
<td>9</td>
<td>Latest PDR/RTC Report Submitted to the ECD</td>
<td>CA, PL, PA</td>
<td>Yes</td>
</tr>
<tr>
<td>10</td>
<td>Latest Access Authorization Documents</td>
<td>RC, RL, PL</td>
<td>Yes</td>
</tr>
<tr>
<td>11</td>
<td>Security Policy [Revised]</td>
<td>CP, CM, CM</td>
<td>Yes</td>
</tr>
<tr>
<td>12</td>
<td>Any WI (Requests to OBA)</td>
<td>CA, SI</td>
<td>Yes</td>
</tr>
<tr>
<td>13</td>
<td>Information Security Continual Monitoring Plan (ICMCMP)</td>
<td>EA, PA, PM</td>
<td>Yes</td>
</tr>
</tbody>
</table>

Security Control List

- Sampling NIST Control/Enhancement
  - Access Control
  - Audit and Accountability
  - Security Assessment and Authorization
  - Configuration Management
  - Contingency Planning
  - Identification and Authentication
  - Incident Response
  - Physical and Environmental Protection
  - Planning
  - Program Management
  - Risk Assessment
  - System and Services Acquisition
  - System and Communications Protection
  - System and Information Integrity

Interview Questionnaire
Results: Metrics

Residual Risk Metrics

Control Compliance Results

Key Performance Area Measurements

<table>
<thead>
<tr>
<th>KPA 1.1: Completeness</th>
<th>KPA 1.2: Quality</th>
<th>KPA 2.1 Education, Training &amp; Certification</th>
<th>KPA 2.2 Experience &amp; Proficiency</th>
<th>KPA 2.3: Security Knowledge &amp; Technical Expertise</th>
<th>KPA 3.1 Controls Review &amp; Assessment</th>
<th>KPA 3.2: Adherence to NIST standards</th>
</tr>
</thead>
<tbody>
<tr>
<td>Initial</td>
<td>Initial</td>
<td>Initial</td>
<td>Initial</td>
<td>Initial</td>
<td>Initial</td>
<td>Initial</td>
</tr>
<tr>
<td>Defined</td>
<td>Defined</td>
<td>Defined</td>
<td>Defined</td>
<td>Defined</td>
<td>Defined</td>
<td>Defined</td>
</tr>
<tr>
<td>Managed</td>
<td>Managed</td>
<td>Managed</td>
<td>Managed</td>
<td>Managed</td>
<td>Managed</td>
<td>Managed</td>
</tr>
<tr>
<td>Optimized</td>
<td>Optimized</td>
<td>Optimized</td>
<td>Optimized</td>
<td>Optimized</td>
<td>Optimized</td>
<td>Optimized</td>
</tr>
</tbody>
</table>
Results: Findings

8 findings common across most of the boundaries were tied to the GRC framework

**Governance**
- Lack of adherence to PBGC policies based on NIST standards
- Lack of coordination of effort across the various stakeholders
- Lack of monitoring and managed oversight for identified risks

**Risk**
- System security processes are not based on NIST RMF
- POA&Ms are incomplete, do not fully detail risks, & have unrealistic timelines
- Lack of comprehensive continuous monitoring

**Compliance**
- Conflicting information provided in the system security documentation
- Incomplete information in the system security documentation
Results: Recommendations

Establish an **Information Security Strategic Plan** focused on enhancing security across department

Ensure true comprehensive **ISCM**, Replacing the point-in-time SA&A process for all systems

Develop a Comprehensive Program **Information Security Architecture**, including defining control mapping for all systems

Refine **Information Security Structure** & alignment of resources

Improve **Communications** & enhance consolidated **project management**
Implementation: Standards

Personnel

• Staff is all full-time dedicated security professionals
• Added security related measures to performance standards
• Training & Certification requirements

Security & Risk Management

• All systems have achieved on-going authorization status
• All systems have completely full control assessment under 800-53 Rev. 4
• All systems have implemented risk based approach to ISCM planning to ensure alignment of work activities and analysis
• All department risk have been properly documented via business impact assessments, risk acceptances, and POAMs as applicable
Implementation: Metrics

- **POA&M Status Summary**:
  - Completed: 130
  - Cancelled: 1
  - Delayed: 4
  - In Progress: 4
  - Planned/Pending: 9

- **Closed POA&M Trending**:
  - 31 Mar 2016: 16
  - 30 Jun 2016: 16

- **Risk Tolerance**
  - In Q3, the adjusted risk over all systems improved from 0.5556 to 0.5079.
  - Contributing factors include:
    - Closure of 20 POA&M
    - Implementation of an organization-wide Incident Response Plan
  - Although many of the POA&M controls are not fully implemented, there are measures in place (e.g., Splunk has been implemented for auditing) to provide a degree of risk remediation. Several control families are implementing portions of each control, which will serve to mitigate some risk to the information systems.
Implementation: Project Management

Information Security Risk Management Program

- Integrated ISSO role into Tier 2 organization
- Defined & appointed ISSM
- Documented roles & responsibilities for security team

Communications

- Schedule & planning for different management reports
- Clarified purpose & scope for various documentation

Processes, Procedures, & templates established

- Created templates & documentation standard for all key deliverables
- ISCM plan based on RMF used by all security teams
- Risk Management process with procedures for: Business Impact Assessment (BIA), Risk Acceptance (RA), & POAM
Implementation: Future

Personnel

• Staff will be placed under GS 2210 series
• All security staff will be professionally certificated by end of FY2017
• Staff realignment due to modernization / decommissioning of systems in FY2018

Program

• Approval of 3 year strategy plan for security program in early FY2017
• Gap analysis on vendor management in FY2017
• Develop a budget forecasting model for security cost in FY2017
• Ongoing maturation of existing security processes & procedures; Development of additional processes & on-line publication starting in FY2017
• Shared business services boundary analysis in FY2018
Questions?