IG Metrics: Maturity Model and the New IG FISMA Assessment Approach

John Ippolito CISSP, PMP
Consultant
Mary Harmison CPA, Audit Manager
Office of Inspector General
Federal Trade Commission
Federal Information Security Modernization Act (FISMA) of 2014
Replaced
Federal Information Security Management Act (FISMA)
Each evaluation under this section shall include:

**2002 FISMA**

- “(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency’s information systems;
- (B) an assessment (made on the basis of the results of the testing) of compliance with
- (i) the requirements of this subchapter; and
- (ii) related information security policies, procedures, standards, and guidelines.”

**FISMA Modernization Act**

- “(A) testing of the effectiveness of information security policies, procedures, and practices of a representative subset of the agency’s information systems;
- (B) an assessment of the effectiveness of the information security policies, procedures, and practices of the agency.”
NIST 800-53 Definition of Effectiveness

Security control effectiveness addresses the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the information system in its operational environment.”
Proposed IG ISCM Maturity Model

**ISCM Attributes**

1.1.1 Documented policies and procedures for ISCM
1.1.2 Documented strategy for ISCM that includes consideration of risk assessments
1.1.3 Implementation of ISCM for IT assets and performance of security controls assessment
1.1.4 ISCM reporting

**Level 1 Ad-hoc**
- ISCM policies, procedures, and strategy not formalized; ISCM activities performed in an ad-hoc, reactive manner

**Level 2 Defined**
- ISCM policies, procedures, and strategy are formalized and documented but not consistently implemented

**Level 3 Consistently Implemented**
- ISCM policies, procedures, and strategy are consistently implemented and agency performs validation testing. However, quantitative and qualitative effectiveness measures are lacking

**Level 4 Managed & Measurable**
- Quantitative and qualitative measures on the effectiveness of ISCM policies and procedures are collected across the organization and used to assess the ISCM program and make necessary changes

**Level 5 Optimized**
- ISCM policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.
### ISCM Maturity Model for FY2015 FISMA

#### 5 level scale across 3 domains

<table>
<thead>
<tr>
<th>Scale/Domain</th>
<th>People</th>
<th>Processes</th>
<th>Technology</th>
</tr>
</thead>
<tbody>
<tr>
<td>1 - Ad-hoc</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2 - Defined</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>3 - Consistently Implemented</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>4 - Managed and Measurable</td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>5 - Optimized</td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Level 2
Assess the skills, knowledge, and resources needed to effectively implement an ISCM program. Develop a plan for closing any gaps identified.

Level 3
Implement plans to close any gaps in skills, knowledge, and resources required to successfully implement an ISCM program. Personnel possess the required knowledge, skills, and abilities to effectively implement the organization’s ISCM program.

Level 4
Consistently implement, monitor, and analyze qualitative and quantitative performance measures across the organization and collect, analyze, and report data on the effectiveness of the organization’s ISCM program.

Level 5
Ensure assigned personnel collectively possess a high skill level to perform and update ISCM activities on a near real-time basis to make any changes needed to address ISCM results based on organization risk tolerance, the threat environment, and business/mission requirements.
Demonstrate training effectiveness of training material

Demonstrate training effectiveness

- Elimination of training GAPS
- Adapts to change

Quantitative vs Qualitative measures