Office of Inspector General Reviews under the Federal Information Security Management Act (FISMA)

Information Security and Privacy Advisory Board

October 10, 2012

Andy Patchan
Associate Inspector General for
Audits and Attestations
Federal Reserve Board of Governors

OIG Responsibilities Under FISMA

- OIGs are required by FISMA to perform an annual evaluation to determine the effectiveness of their agency’s information security program and practices

  - Testing of the effectiveness of information security policies, procedures, and practices of a subset of the agency’s information systems
  - An assessment of compliance with FISMA requirements and related information security policies, procedures, standards, and guidelines

FISMA Provides a Structured Process for Assurance of Information Security

- Risk assessments of the risk and magnitude of the harm that could result from unauthorized access, use, disclosure, disruption, modification, or destruction of information or systems
- Policies, procedures, and security plans that determine controls needed to cost-effectively reduce risks to an acceptable level
- Periodic testing and evaluation of the effectiveness of policies, procedures and controls

FISMA Provides a Structured Process for Assurance of Information Security (cont.)

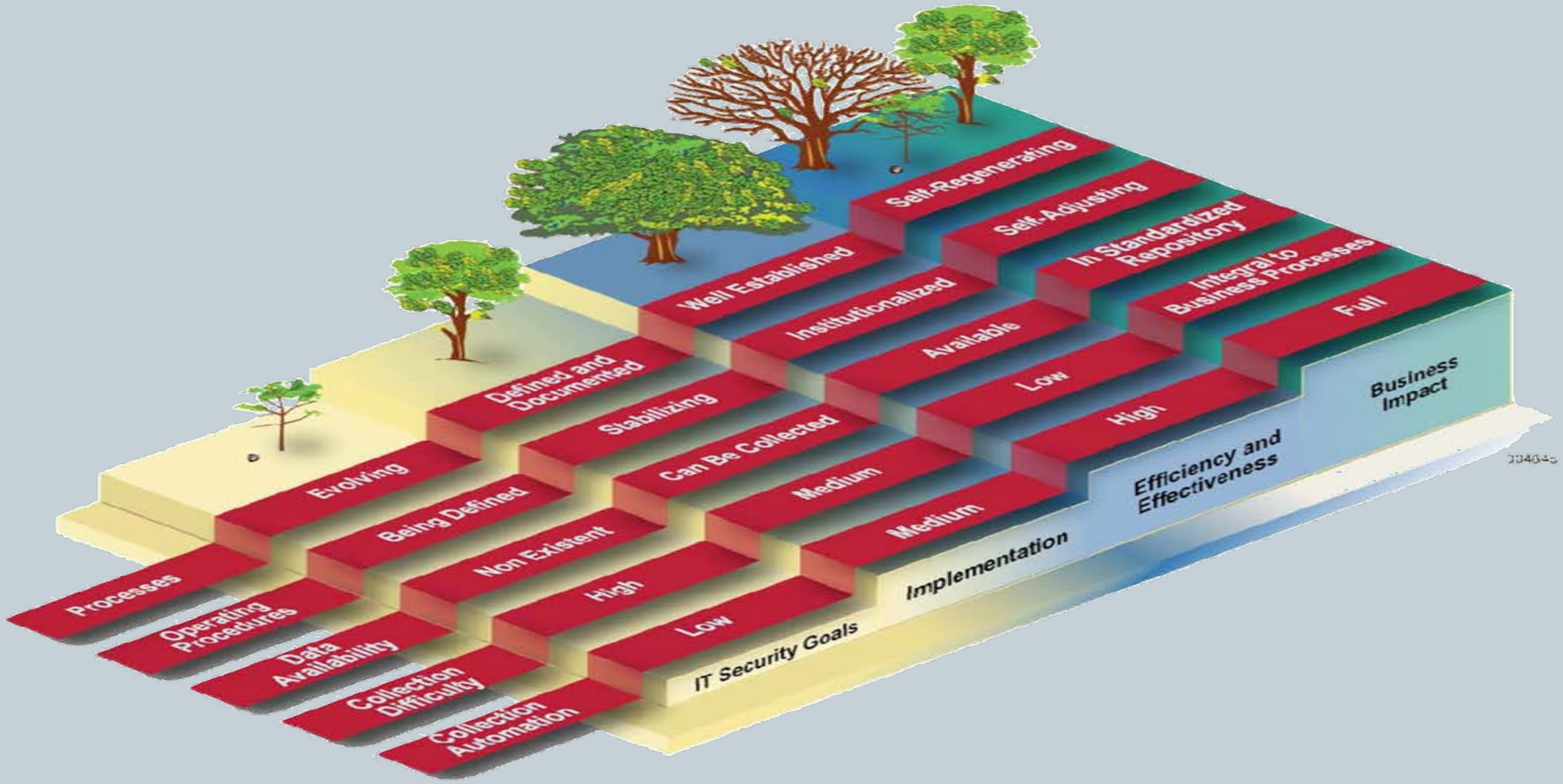
- Process for planning, implementing, evaluating, and documenting corrective actions to address deficiencies
- Security awareness training
- Procedures for detecting, reporting, and responding to security incidents
- Plans and procedures for ensuring continuity of operations of information systems

2012 FISMA Reporting Metrics for IGs

- DHS FISMA guidance directs the OIGs to focus their reviews on:
  - Risk management
  - Continuous monitoring
  - Incident response and reporting
  - Security training
  - Plan of actions and milestones
  - Remote access management
  - Identity and access management
  - Configuration management
  - Contingency planning
  - Contractor systems
  - Security capital planning

Measuring the Maturity of Agency Information Security Programs, Policies, and Procedures

NIST Maturity Model


Processes
Evolving
Defined and Documented
Well Established
Self-Regenerating
Operating Procedures
Being Defined
Stabilizing
Institutionalized
Self-Adjusting
Data Availability
Non Existent
Can Be Collected
Available
In Standardized Repository
Collection Difficulty
High
Medium
Low
Integral to Business Processes
Collection Automation
Low
Medium
High
Full
IT Security Goals
Implementation
Efficiency and Effectiveness
Business Impact