IT Security Technical Testing Panel

Federal Audit Executive Council
2018 Annual Conference

Council of the Inspectors General on Integrity and Efficiency

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Khalid Hasan
Don Patterson

September 4, 2018

Overview

- Federal Information Security Modernization Act of 2014 (FISMA)
- Information Technology (IT) audit testing lab at our OIG
- Challenges and lessons learned in operating an IT audit test lab

FISMA of 2002 vs. FISMA of 2014

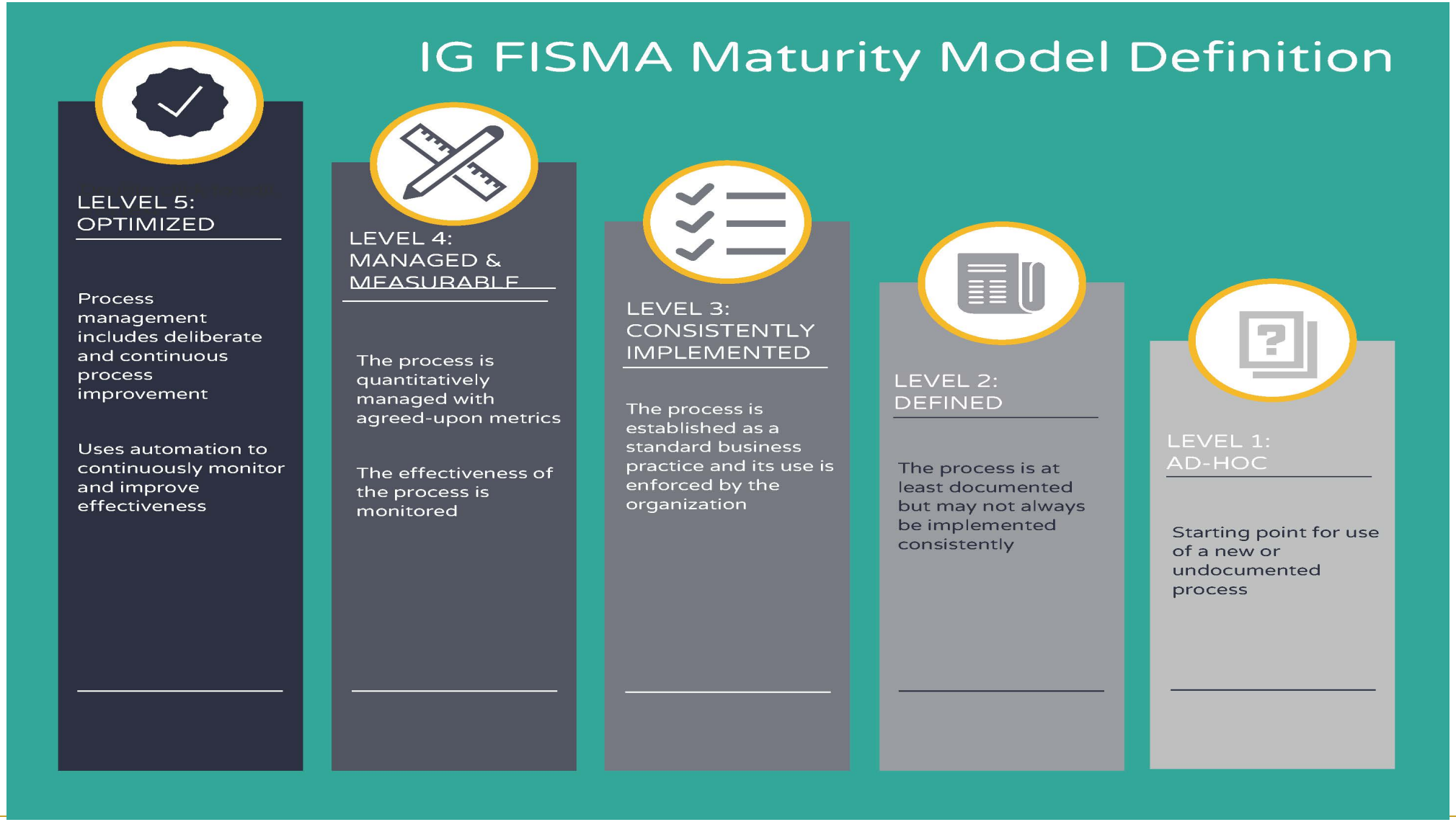
FISMA of 2002

- Perform an annual independent evaluation of information security program and practices
  - Testing effectiveness of policies and procedures for subset of systems
  - An assessment of **compliance** with FISMA and related policies, procedures, standards, and guidelines

FISMA of 2014

- Perform an annual independent evaluation of information security program and practices
  - Testing effectiveness of policies and procedures for subset of systems
  - An assessment of **the effectiveness** of the information security policies, procedures, and practices of the agency

IG FISMA Maturity Model



IT Audit Test Lab

- Lab is not connected to the agency's network
- Largely consists of excessed equipment from the agency and our OIG
- Used as a testing ground to train auditors on technologies and tools in a safe environment
- Mix of free/open source and commercially available tools

Select Free/Open Source Tools in our Lab

Security Testing Tool	Audit Use Cases
Nmap	Verify inventory of devices; analyze services and programs running and compare against those that are authorized
Nessus*	Audit device configurations against organization hardening guides
Kismet, Netstumbler, Aircrack, wififisher	Verify authorized wireless connection points, security protocols in use, test strength of encryption keys
Burp Suite**	Identify vulnerabilities in web applications
Rkhunter	Vulnerability scanner for Unix/Linux based systems that can identify backdoors, rootkits

*Nessus is free for personal use in a home environment; annual cost for organizations is approx. $2k
** Burp suite community edition is free; professional version approx. $500/year

Commercially Available Tools in our Lab

Security Testing Tool	Audit Use Cases
Nexpose	Vulnerability scanning and exploitation using Metasploit;
SAINT	Vulnerability scanning and conducting phishing tests
AppDetective Pro	Database-level vulnerability scanning and user rights reviews

Open Source and Dark/Deep Web Intelligence

- Open Source Intelligence
  - Pastebin
  - Sensitive documents using google
  - https://inteltechniques.com/osint

- Dark/Deep Web Intelligence
  - FinCen services
  - Search tools

Challenges and Lessons Learned

- Recruiting and retaining individuals with the right expertise
  - Have utilized OPM's CyberCorps: scholarship for service program
  - Offering an IT audit career track for those interested in more technical testing/ managing the lab with a defined career ladder
  - Rethinking traditional audit reporting
- Communicating the value of the lab internally and to agency management
  - Created a concept of operations and rules of engagement
- Budget considerations
  - Start by using open source tools to build a business case
  - Utilize excessed equipment

HHS OIG Cyber Assessment Capabilities

- Vulnerability Scanning (web, database, wireless, network)
- Cyber Threat Intelligence Gathering
- Reconnaissance / OSINT
- Penetration Testing (internal, external, wireless, social)
- Red Teaming
- Cyber Threat Hunting and IOC assessments
- State-of-the-art Cyber Range Lab
- IT Audit Software and Hardware
- Cyber Exploit and Defense Training

Building Technical Testing Capabilities: Level I

- Strategic Plan outlined – include tactical goals
- Identify initial staff resources – gauge their potential
- Identify and document current technical resources and gaps
  - Tools – open source, COTS
  - Network communications – separate ISP, 4G LTE
  - Training – Windows, Linux, command line, networking, web
  - Cyber Range / Test Lab
- Select a potential target system – draft a concept RoE
- Partner with an internal or external SME
- Formulate initial budget
- Engage Executive Sponsors and communicate ROI

Building Technical Testing Capabilities: Level II

- Strategic Plan fully documented
- Draft business plan and future budget projections
- Executive Level Sponsor identified to champion
- Initial resource gaps addressed (people, funding, tools)
  - Procure needed software, hardware, network communications
  - Technical training provided as needed
- Conduct initial pilot technical assessment(s); low complexity
- Lessons learned reviewed and addressed, guidelines created
- Shore up gaps (e.g. additional training, process improvements)
- Integrate technical testing techniques into IT Audits

Building Technical Testing Capabilities: Level III

- New targets identified; higher complexities
- Managed software and hardware procurement process
- Technical resources being utilized more frequently
- Technical testing techniques or audit programs documented
- Executive Level Sponsor communicating results and needs to the stakeholder community frequently
- Cyber Testing Range / Lab ConOps and business case
- Technical knowledge being shared, cross-pollination

Building Technical Testing Capabilities: Level IV

- Repeatable processes, work flows, shared templates
- Collaborative communication methods in place
- Continued Investment / Budget
- Cyber Testing Range / Lab fully operational and ATO
- Staff resources independently demonstrating subject matter expertise
- Recruitment plan – attract and retain
- Continual Research and Training to improve staff skills
- Optimal resources in place (people, funding, tools)

Questions?