

Getting to Green – Five Opportunities for Improvement in FISMA

August, 2011



Antione Manson

Federal Network Security (FNS) Branch

Department of Homeland Security



Homeland
Security

Federal Network Security
August, 2011 – GFIRST Conference

Abstract

- Presenter: Antione Manson, Program Manager, Federal Network Security Branch, National Cyber Security Division, DHS
- Agency FISMA scores are important and highly publicized measures of the state of cyber security in the Government. However, FISMA scores are determined based upon answers to a small number of questions. This presentation will introduce a diagnostic questionnaire-based instrument that focuses on five areas that most closely align with FISMA.



Purpose and Outcomes

- Purpose:

Introduce the services offered by FNS-Security Management and discuss their basis

- Outcomes

- The four categories of assets.
- The four classes of operational risk.
- The five process areas that most heavily influence FISMA scores.
- Why applying technology is not enough to combat ever-increasing threats and vulnerabilities.
- Why vulnerabilities are only part of the risk assessment equation.
- How to apply a questionnaire-based survey to quickly diagnose performance in these five areas.

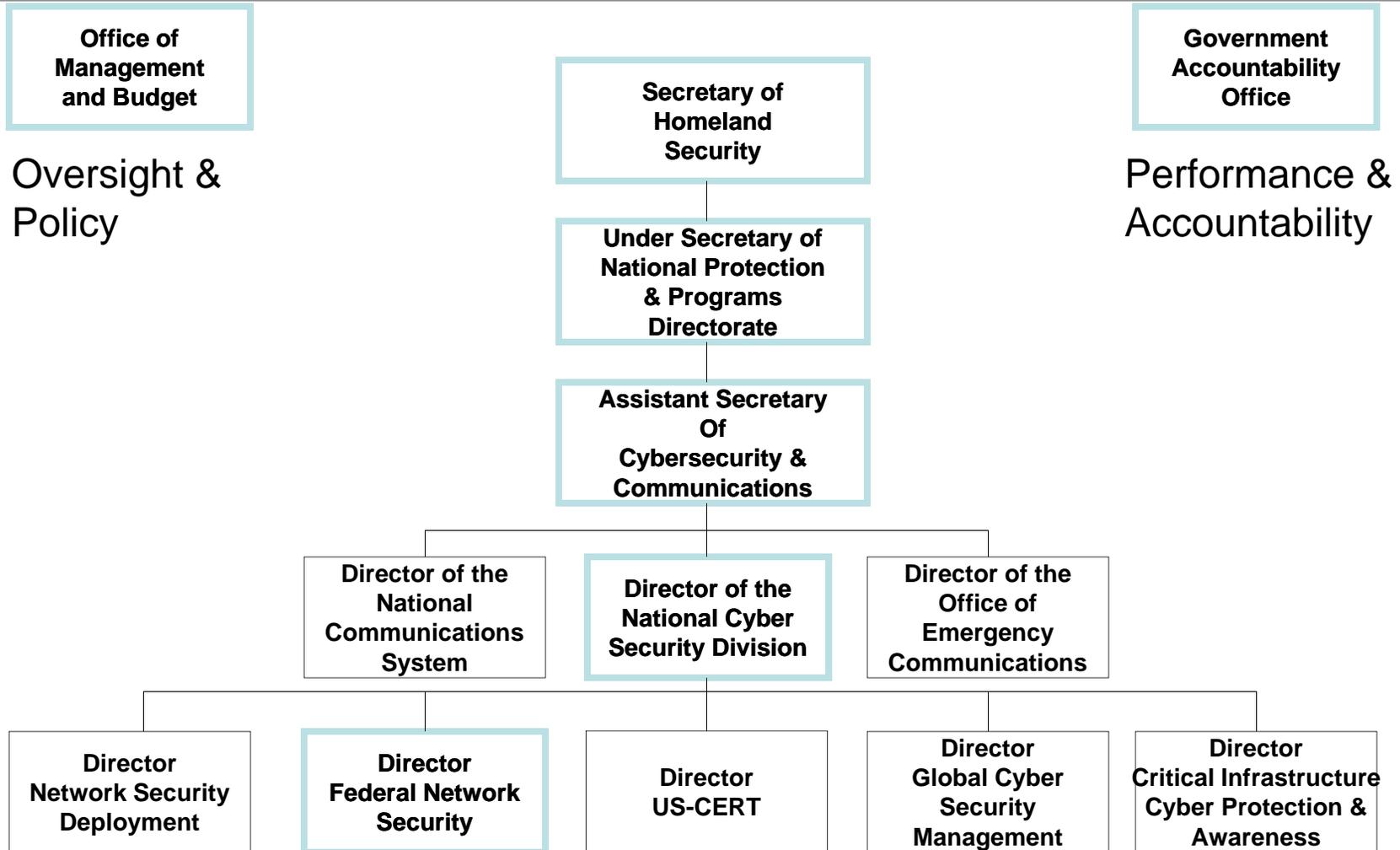


Federal Network Security (FNS)

- Assigned as the executive agent for Office of Management and Budget (OMB) cybersecurity initiatives and FISMA reporting (OMB Memo M-10-28)
- National program, part of the DHS National Cyber Security Division (with US-CERT, NSD, etc)
- Focused on providing the means to enable long-term strategic prevention of attacks against federal government networks by addressing common challenges faced by all Federal civilian agencies
- FNS works with all Federal Executive Branch civilian agencies (.GOV)
- FNS does not manage or procure IT network services

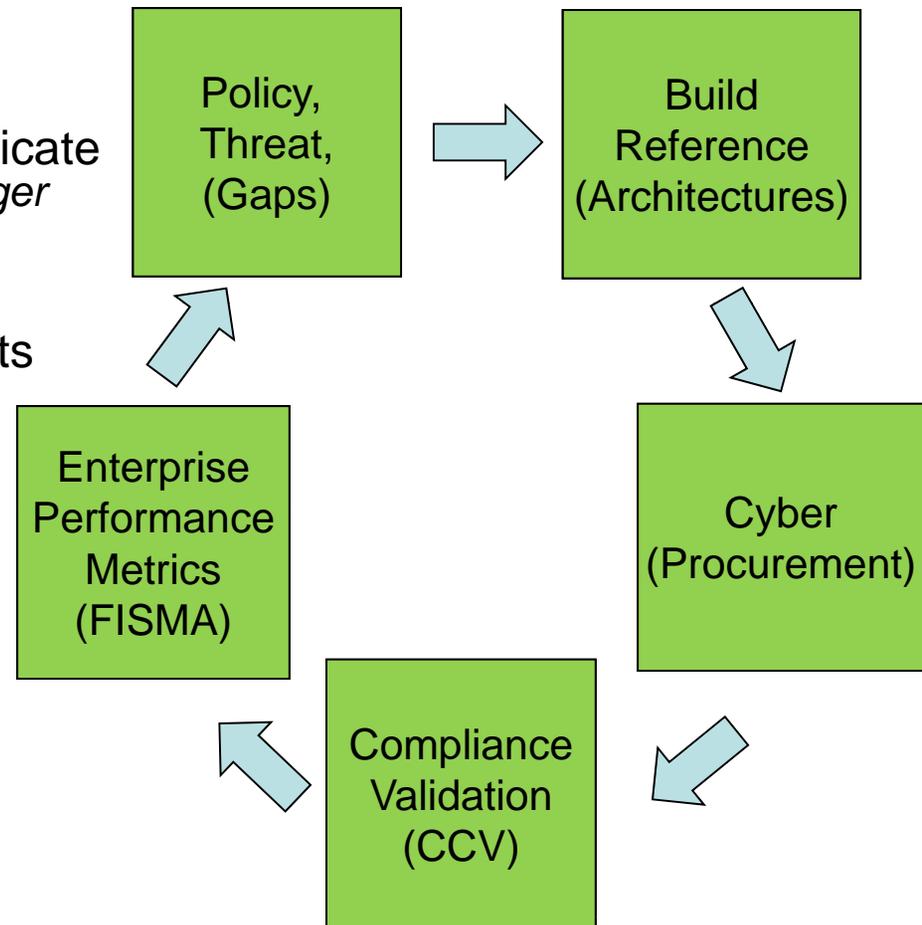


Federal Network Security (FNS)

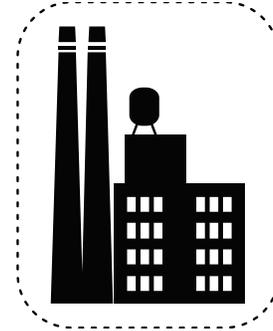
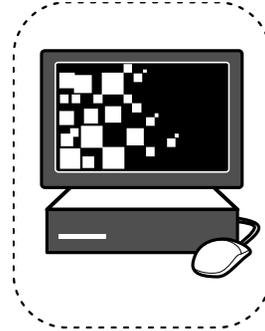
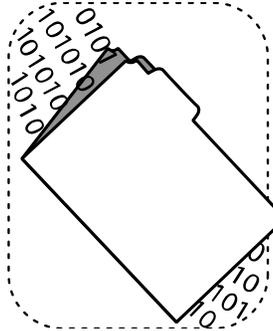
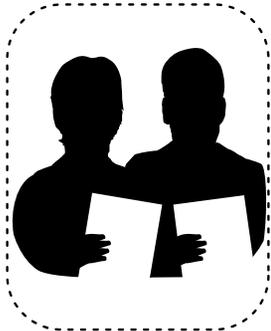


FNS in Cyber Community

- Identify threats, gaps or opportunity
e.g. Informs policy development
- Policy prompts opportunity to communicate
e.g. Informs information sharing; forums, tiger teams, conferences
- Data sharing drives cyber procurements
e.g. Informs procurement requirements process
- DHS validates agency compliance
e.g. CCV assessments
- Agencies submit enterprise performance metrics
e.g. FISMA Boundary Protection Section



Assets

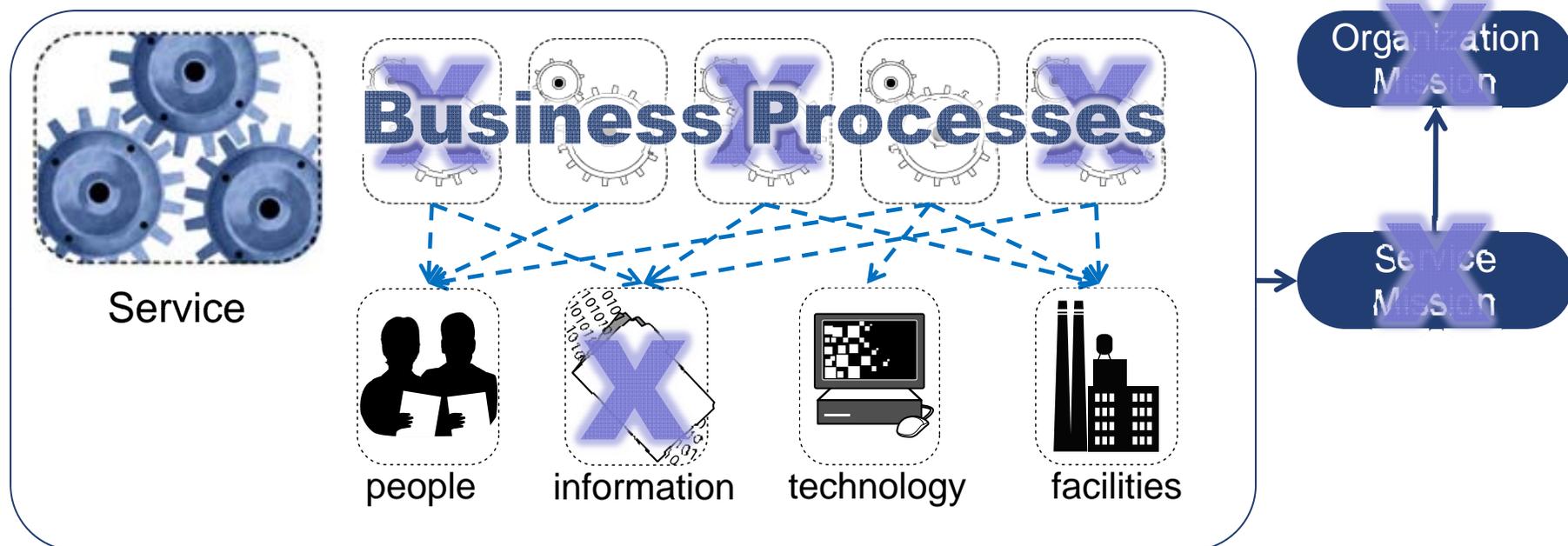


Four types of assets are considered in operational risk management. These include **people, information, technology, and facilities.**

Management of *operational cyber security risks* is directly focused on information and technology assets. People and facility assets are considered to the extent that they support information and technology.



Impact of disrupted asset on service mission



The failure of one or more assets has a cascading impact on the mission of related **business processes**, **services**, and the **organization** as a whole.



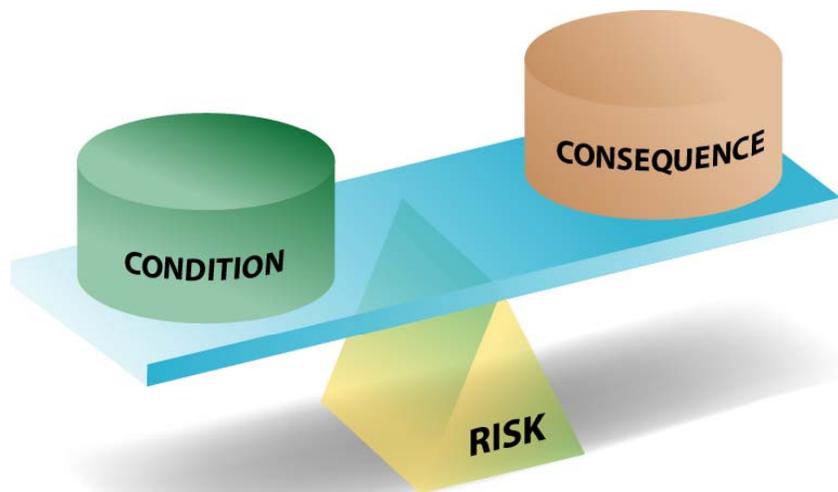
Protection and sustainment

- The strategies developed to identify, develop, implement, and manage controls commensurate with an asset's resilience requirements
- **Protection strategies** address how to minimize the asset from exposure to threats and vulnerabilities.
- **Sustainment strategies** are continuity-focused—address how to
 - keep the asset operable when adversely affected or
 - how to keep an associated business process or service operable without the asset's contribution
- **Each asset needs an optimal balance of these strategies.**

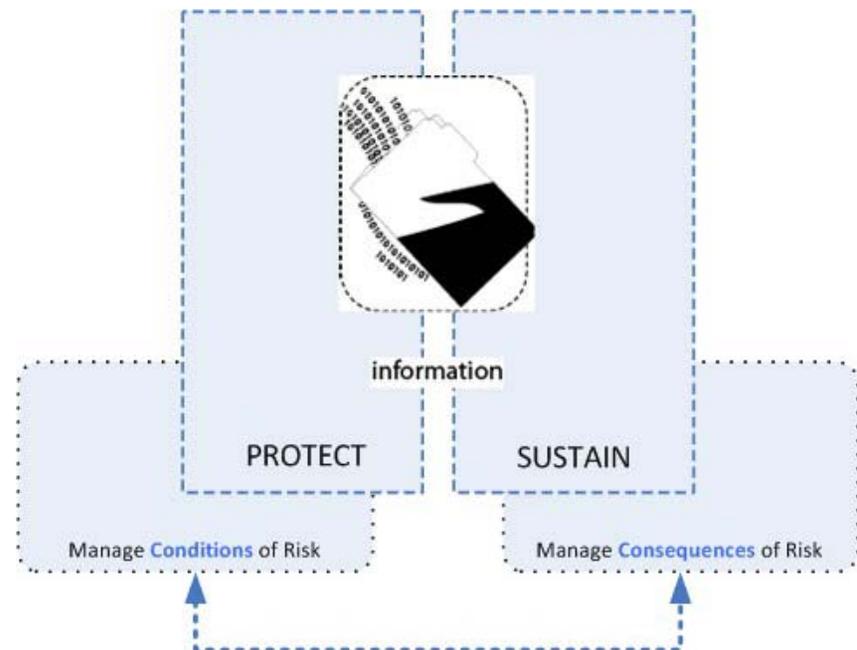


Protection, sustainment, and risk

Basic risk equation



Protection & sustainment



Operational risk

- There are four classes of operational risk:



**Actions of
people**



**Systems &
technology
failures**



**Failed
internal
processes**



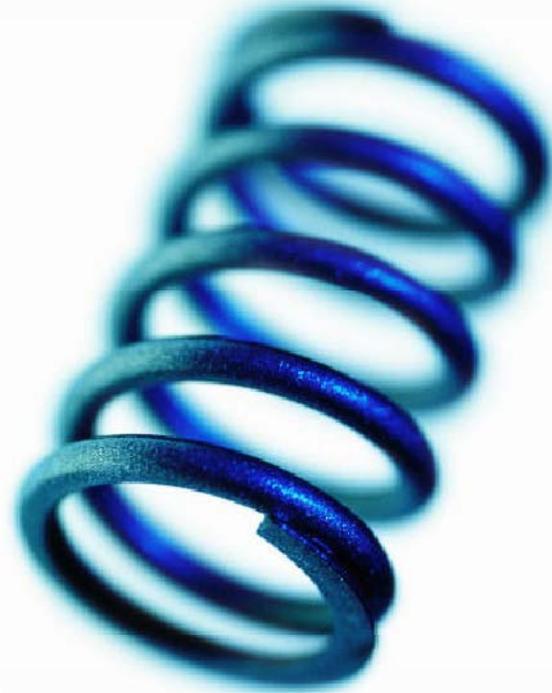
**External
events**



Resilience defined

- The physical property of a material when it can return to its original shape or position after deformation that does not exceed its elastic limit

[wordnet.princeton.edu]



Parsed in organizational (and operational) terms:

*The **emergent** property of an **organization** when it **continues to carry out its mission** after **disruption** that **does not push it beyond its operational limit***



Doing vs. managing

- Most organizations have experience at the tactical level
 - Significant body of **codes of practices** to guide effort
 - Significant range of **technology solutions**
 - Practitioners' **skill levels** have matured significantly
- BUT—very few organizations are skilled at **managing the process** so that it
 - is effective, efficient, optimal, and meets stated objectives
 - can produce reliable and predictable results:
 - now (in the steady state)
 - under times of stress
 - under uncertain conditions
 - when the risk environment changes



Technology-centric approaches

- Fail to recognize that managing operational risk is an organizational problem
- Can be ineffective if they are not actively managed and continuously improved
- Often leave management to ask: “If we have state-of-the-art technologies deployed, why do we still suffer disruptions?”



Move past “vulnerabilities”

- Vulnerability assessment is NOT risk assessment
- Vulnerability assessment is for identifying *conditions*
- Conditions must be taken in the context of the organization’s unique operating circumstances
- There must be a consideration of *consequence* to be meaningful



Move past “controls”

From a recent Government security conference ...

- “The solution is broader than a control catalog”
- “Sites are having trouble with ‘Risk Management’ that is controls based since that leads to a compliance mindset.”
- “The controls and system security activities must be related to a business impact analysis.”



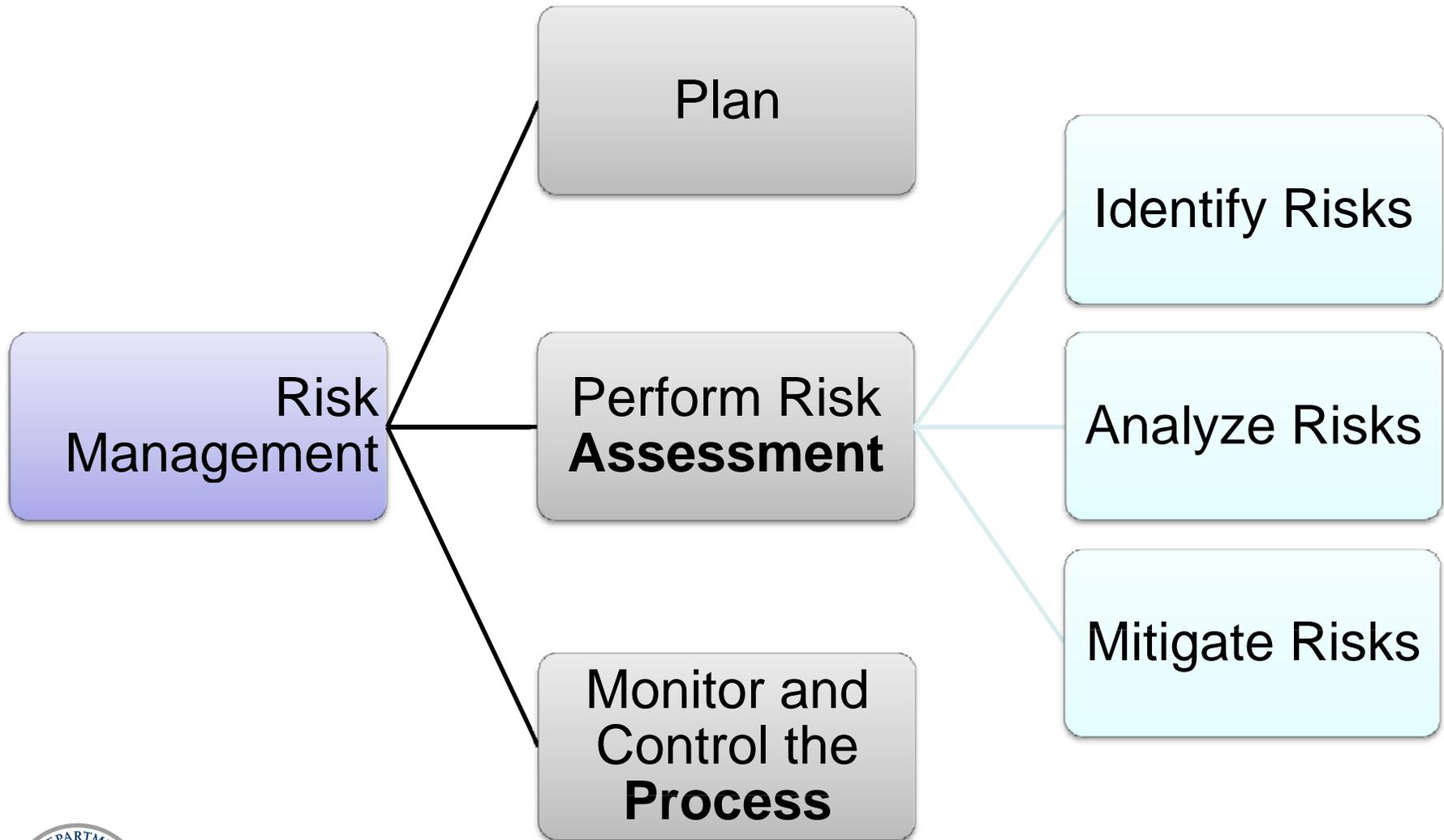
Enterprise Risk Management Perspective

An enterprise view of operational risk management

- Enables risk mitigation decisions that effectively deploy limited resources
- Integrates with enterprise architecture approaches to security management
- Supports NIST SP 800-39's "Risk Executive" function
- Incorporates physical and cyber security management



Risk Management vs. Risk Assessment



Federated Cyber Resilience Management Program (Fed-CRMP)

- Developed by SEI-CERT for DHS-FNS
- Built from published SEI-CERT bodies of work
 - Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE) method
 - CERT Resilience Management Model (CERT-RMM) – 26 process areas
- Tools developed to support the Program
 - Risk Taxonomy (Common description of risks)
 - Diagnostic Assessment Instrument (question based)
 - Process Measurements
 - Implementation (are you doing something)
 - Process Performance (how are you doing it)
 - Efficacy/Effectiveness (is it working)



Features of Fed-CRMP

- Defines a risk taxonomy to provide a common language to describe operational cyber security resilience
- Provides a structured definition of operational cyber security risks
- Builds upon a “risk ecosystem” – a group of related business process areas that impact resilience
- Enables sustainable and efficient compliance through streamlined efforts and controls
- Provides a roadmap for establishing and maturing your resilience management program



How the Fed-CRMP Assessment Works

- Pre and post questionnaire based assessments
 - Pre-assessment scoping done by conference bridge and facilitated by FNS-SM (choose the process areas of interest)
 - Assessment questionnaire completed on site in a facilitated workshop.
- Expert help provided by the Fed-CRMP team composed of DHS and CERT staff. Funded by DHS.
- Reports and follow-up support provided at the end of each assessment phase.
- Typically two 1-2 day onsite visits, ~2 mos. Elapsed time



Fed-CRMP Risk ecosystem

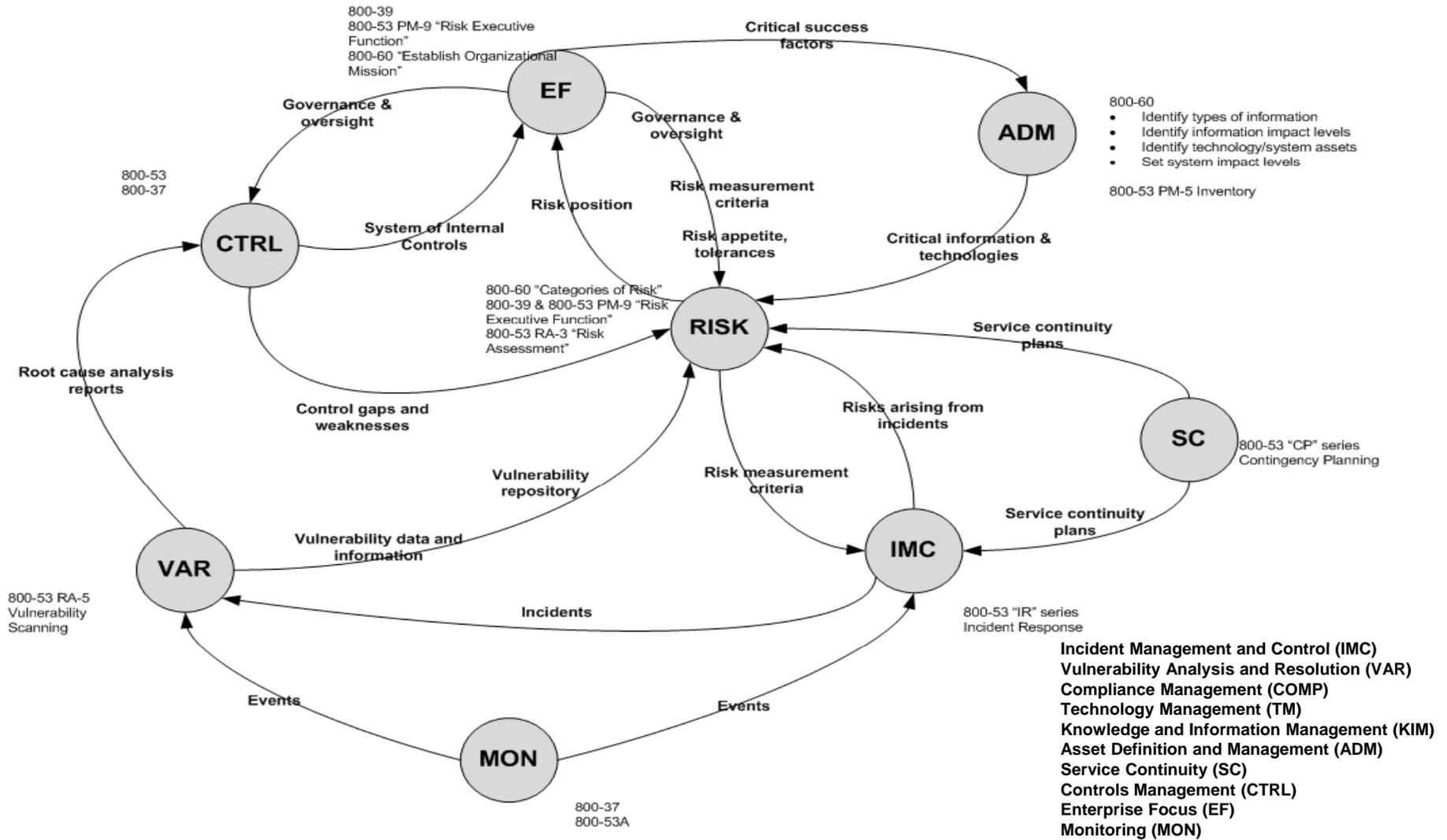
- **Incident Management and Control (IMC)**
- **Vulnerability Analysis and Resolution (VAR)**
- Compliance Mgmt. (COMP)
- Technology Management (TM)
- **Knowledge and Information Management (KIM)**
- **Asset Definition and Management (ADM)**
- Service Continuity (SC)
- Controls Management (CTRL)
- Enterprise Focus (EF)
- **Monitoring (MON)**

The BOLD process areas most closely align to the FISMA metrics

The complete set provide a holistic view of risk management



Risk Ecosystem example



Fed-CRMP Pilots

- Two pilots have been conducted
 - Written reports and senior management briefings provided
 - Successes:
 - One agency used findings to inform department wide risk management policy
 - One agency used results to drive two process improvement projects
- Other engagements planned



We Also Offer ...

Security Management Maturity Questionnaire (SMMQ)

- Lightweight questionnaire that can be self-administered
- Examines maturity of security program management practices across several domains
- Experience has shown that maturity in security program management correlates with higher FISMA scores



We Need You

- FNS-SM is seeking agency participation
 - Fed-CRMP assessments
 - SMMQ Survey participants
- **No Direct Cost to Agencies**



Contact Information

Antione Manson

Program Manager, Security Management
Federal Network Security Branch

FNS.SM@hq.dhs.gov



Homeland
Security

Federal Network Security
August, 2011 - GFIRST Conference

Disclaimer

- © 2011 Carnegie Mellon University
- Except for the U.S. government purposes described below, this material SHALL NOT be reproduced or used in any other manner without requesting formal permission from the Software Engineering Institute at permission@sei.cmu.edu.
- This work was created with the funding and support of the U.S. Department of Homeland Security under the Federal Government Contract Number FA8721-05-C-0003 between the U.S. Department of Defense and Carnegie Mellon University for the operation of the Software Engineering Institute, a federally funded research and development center. The U.S. government's rights to use, modify, reproduce, release, perform, display, or disclose this material are restricted by the Rights in Technical Data-Noncommercial Items clauses (DFAR 252-227.7013 and DFAR 252-227.7013 Alternate I) contained in the above identified contract. Any reproduction of this material or portions thereof marked with this legend must also reproduce the disclaimers contained on this slide.
-
- Although the rights granted by contract do not require course attendance to use this material for U.S. government purposes, the SEI recommends attendance to ensure proper understanding.
-
- THE MATERIAL IS PROVIDED ON AN “AS IS” BASIS, AND CARNEGIE MELLON DISCLAIMS ANY AND ALL WARRANTIES, IMPLIED OR OTHERWISE (INCLUDING, BUT NOT LIMITED TO, WARRANTY OF FITNESS FOR A PARTICULAR PURPOSE, RESULTS OBTAINED FROM USE OF THE MATERIAL, MERCHANTABILITY, AND/OR NON-INFRINGEMENT).
- CERT® is a registered mark of Carnegie Mellon University





Homeland Security



Homeland Security

Federal Network Security
August, 2011 - GFIRST Conference