GFIRST 2012 8th Annual National Conference
August 19-24 | Atlanta Marriott Marquis | Atlanta, Georgia

Leveraging Governance to Enable the Transition to Continuous Monitoring

By Jamie Miller, MBL Technologies

MBL TECHNOLOGIES

This briefing discusses why strong governance mechanisms are necessary to achieve a successful transition to continuous monitoring

Agenda

1. Define Continuous Monitoring
   - How it is Changing the Game of Information Assurance
2. Define Governance in Relation to Continuous Monitoring
3. Identify a Governance Framework to Enable the Transition to Continuous Monitoring
   - Key Components of the Governance Framework

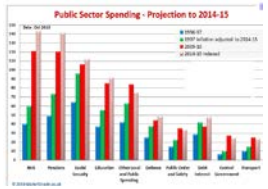
Key Take-Aways

- ✓ Achieve consensus on how/why governance and continuous monitoring are inherently linked
- ✓ Explain why a governance model is needed and the strategic considerations needed to stand-up a continuous monitoring capability
- ✓ Identify the key governance components that are needed to ensure a successful continuous monitoring program

What is Continuous Monitoring?

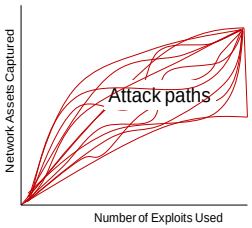
Market Drivers

Reductions to Federal Budget



- The Federal deficit is driving down agency budgets, so pressures to save costs are great

Focus on Real-Time Response



- It is widely agreed that the current security authorization process is inefficient, costly,[1] and does not adequately protect against real-time threats

Federal Guidance – Compliance

- NIST SP 800-137, *Continuous Monitoring for Federal Information Systems and Organizations*

- OMB A-130 and FISMA requirement for near real-time monitoring

Continuous Monitoring Defined

Definition

- Process of leveraging automated tools and technologies and supporting processes to enable the continuous assessment of IT systems, networks, or programs; and capture near real-time security information to effectively and efficiently manage risk, while reducing cost

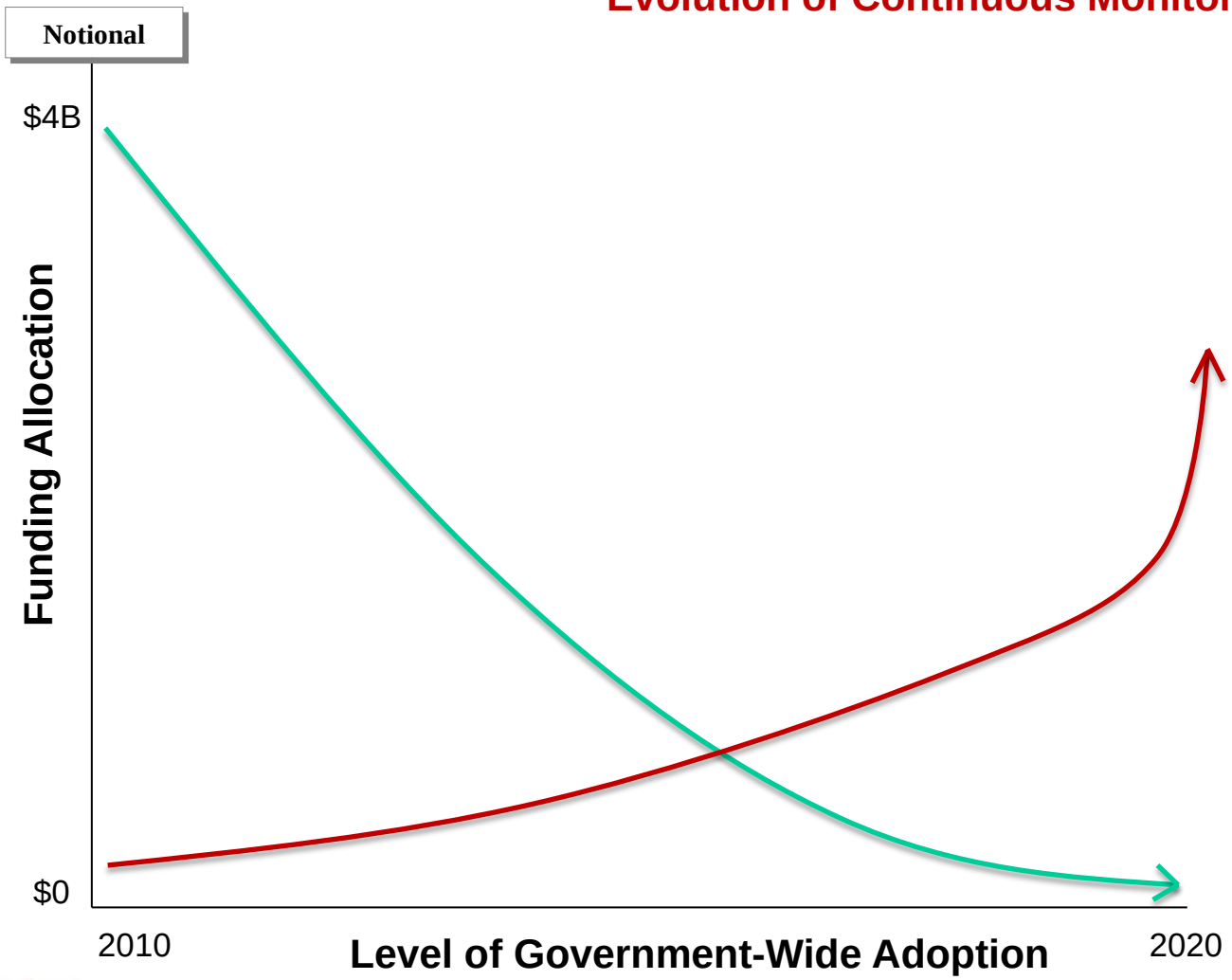
Key Concepts

- Security controls are assessed on a "continuous" basis to provide "near real-time" security posture instead of the traditional "snapshot-in-time" view (i.e., every year to three years)
- Near real-time risk assessment is based on how well security controls mitigate known threats and vulnerabilities (i.e., attack models)
- Enables real-time risk management decision-making

[1]Sen. Tom Carper (D-Del.), chair of the Senate Subcommittee on federal financial management, government information, federal services, and international security, said the C&A process costs taxpayers about $1.3 billion every year.

MBL TECHNOLOGIES

Continuous monitoring is expected to supersede the traditional security authorization process over the next five years



Source: Symantec Internet Security Threat Report, Volume XIII
2011 CSI Computer Crime and Security Survey

"*Near real-time risk management of information systems can be facilitated by employing automated support tools to execute various steps in the RMF including authorization-related activities.*"
SP800-37 Rev 1

MBL TECHNOLOGIES

What is Governance?

Governance Defined

Governance is "the set of responsibilities and practices exercised by the board and executive management with the goal of providing strategic direction, ensuring that objectives are achieved, ascertaining that risks are managed appropriately and verifying that the enterprise's resources are used responsibly" [1]

[1] http://www.itgi.org/Template_ITGI.cfm

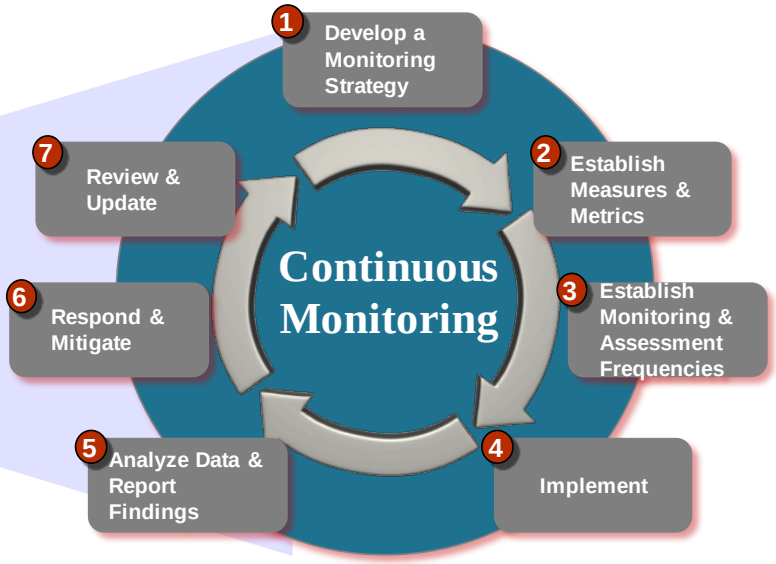
Practical Objectives

Parameters – Organization-defined rules, regulations, and specific requirements that stakeholders must adhere to support their mission…

Control and Oversight – The mechanisms to *continuously monitor* and enforce the practices, processes, and outputs of the organization to ensure they align the required parameters…

Programmatic Enablers – Program processes and functional components that that support the adherence to parameters and align with the organization's mission…

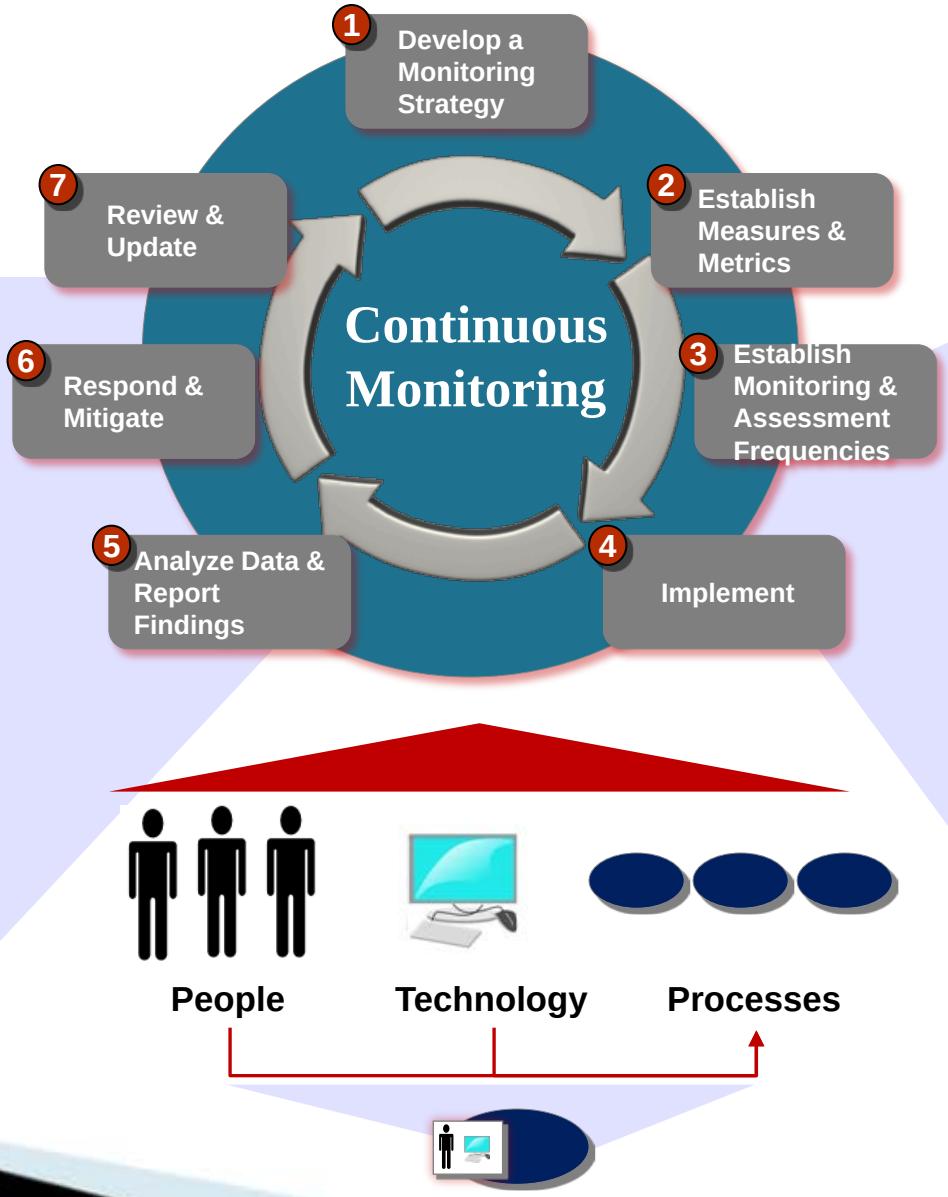
Continuous Monitoring



MBL TECHNOLOGIES

It is important to stress that continuous monitoring is more than just a tool or technology – it is a process that assesses other processes

NIST 800-137 Continuous Monitoring Process



All steps should focus on the five foundational areas where security automation can be most easily attained:

- Asset Mgmt.
- Compliance Mgmt.
- Vulnerability Mgmt.
- Patch Mgmt.
- Malware Mgmt.

Steps where you need to have continuous monitoring tools

BIGFIX

symantec.

TENABLE Network Security

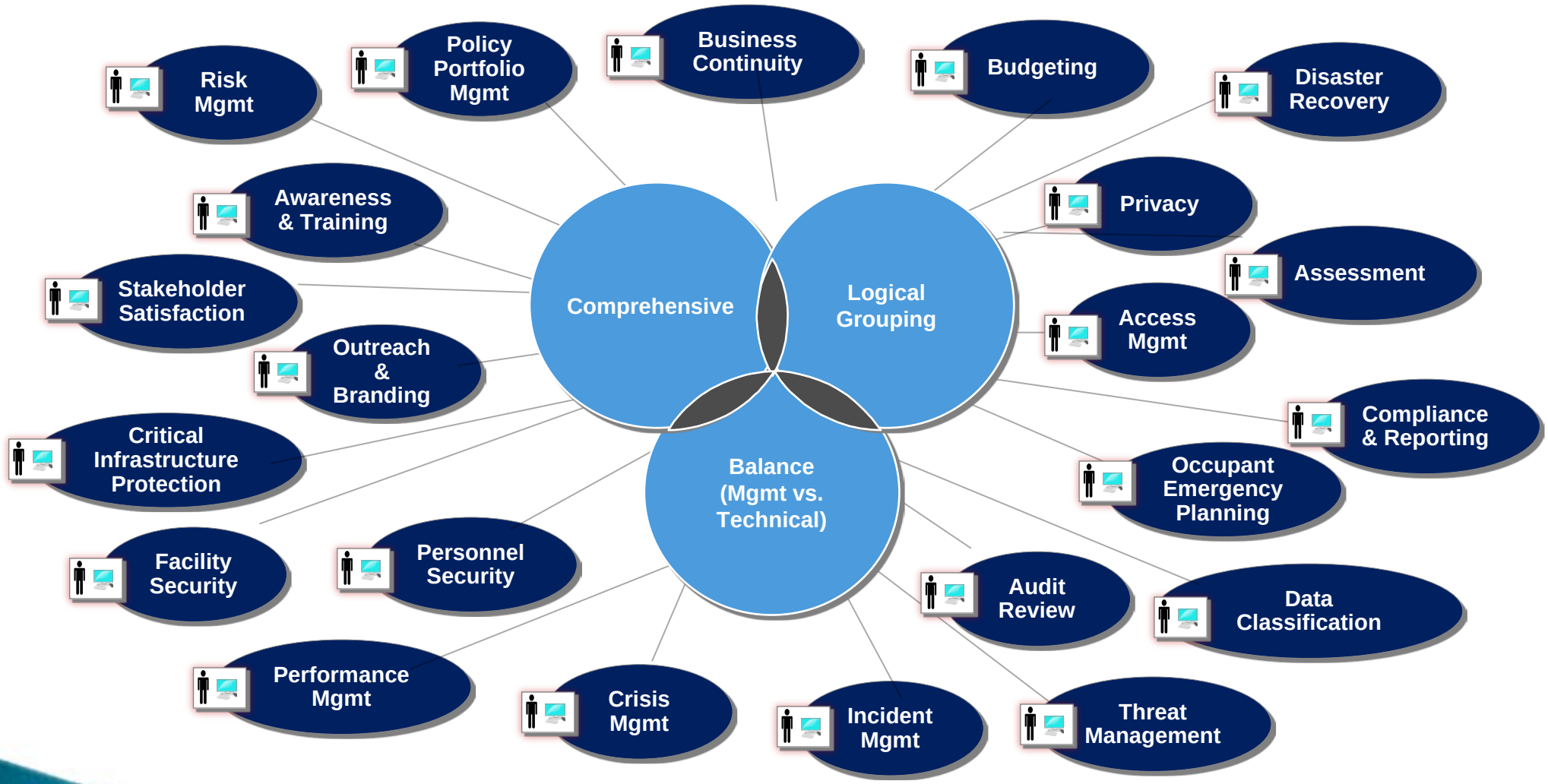
Triumfant

MBL TECHNOLOGIES

In order to establish a continuous monitoring capability it is necessary to first assess the full spectrum of your security processes…

Spectrum of Information Security Governance Processes

ILLUSTRATIVE
(Not Exhaustive)



…and supporting people and technology

MBL TECHNOLOGIES

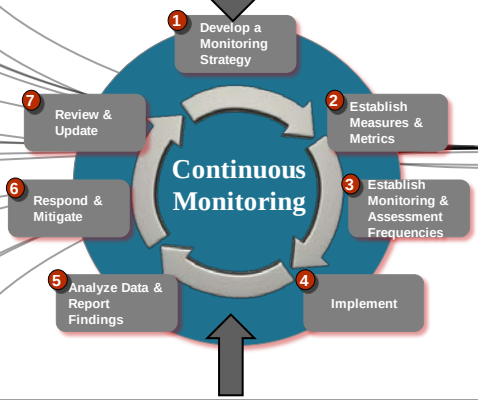
How you organize these components to enable continuous monitoring depends on an effective governance structure/model

Governance Processes

- Stakeholder Satisfaction
- Budgeting
- Risk Mgmt
- Critical Infrastructure Protection
- Crisis Mgmt
- Policy Portfolio Mgmt
- Incident Mgmt
- Audit Review
- Technology Evaluation
- Business Continuity
- Facility Security
- Outreach & Branding
- Assessment
- Disaster Recovery
- Performance Mgmt
- Data Classification

Drivers

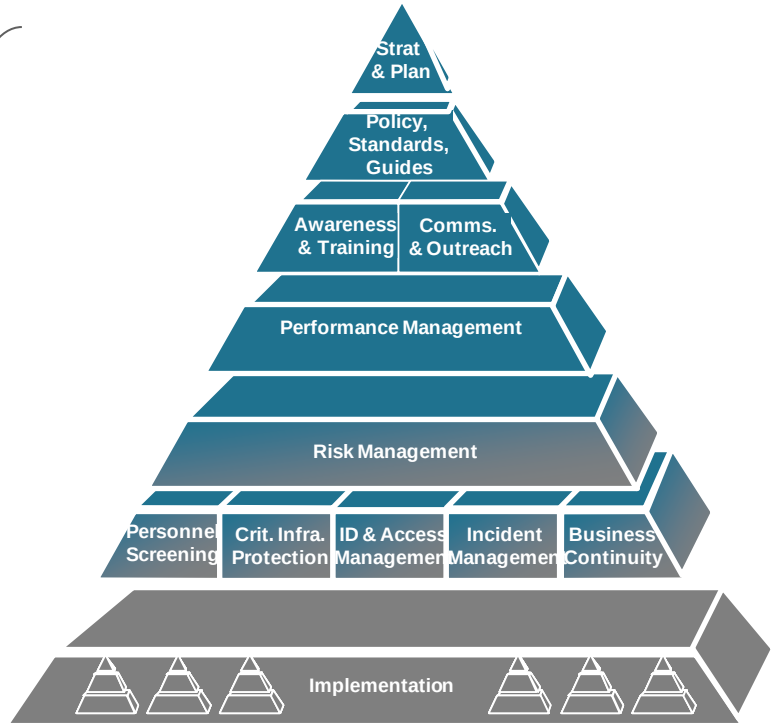
- Compliance with laws and regulations
- Threats and vulnerabilities
- Dependency of and on various organizations
- Business/Mission needs



Challenges

- Organizational design
- Accountability variances
- Tools differentiation
- How and who establishes the risk appetite
- Resource constraints

Governance Model



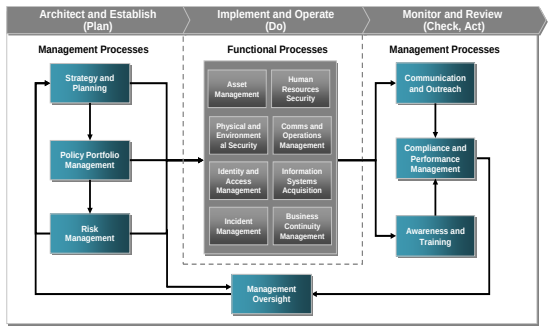
MBL TECHNOLOGIES

There are a variety of information security governance frameworks to aid us in laying the foundation for continuous monitoring

ILLUSTRATIVE
(Not Exhaustive)

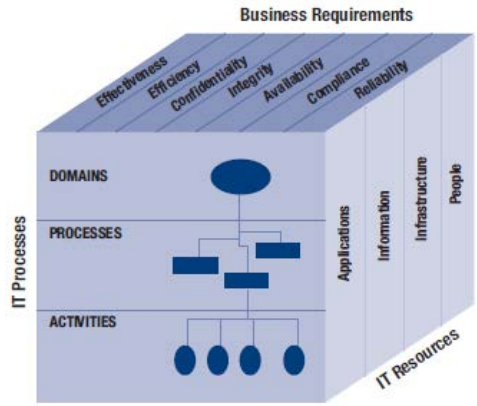
Sample Governance Frameworks

IEC | ISO International Organization for Standardization | COSO | COBIT 4.0 | ITIL | NIST



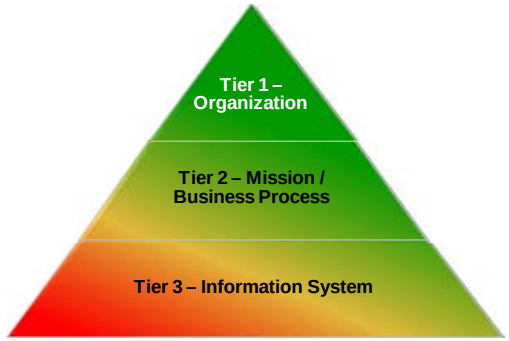
ISO 27001 – ISMS

ISO/IEC 27001 formally specifies a management system that is intended to bring information security under explicit management control (e.g., Plan, Do, Check, Act)



COBIT

COBIT is an IT governance framework that outlines a set of generally accepted measures, indicators, processes and best practices to aid in maximizing the benefits derived through the use of information technology

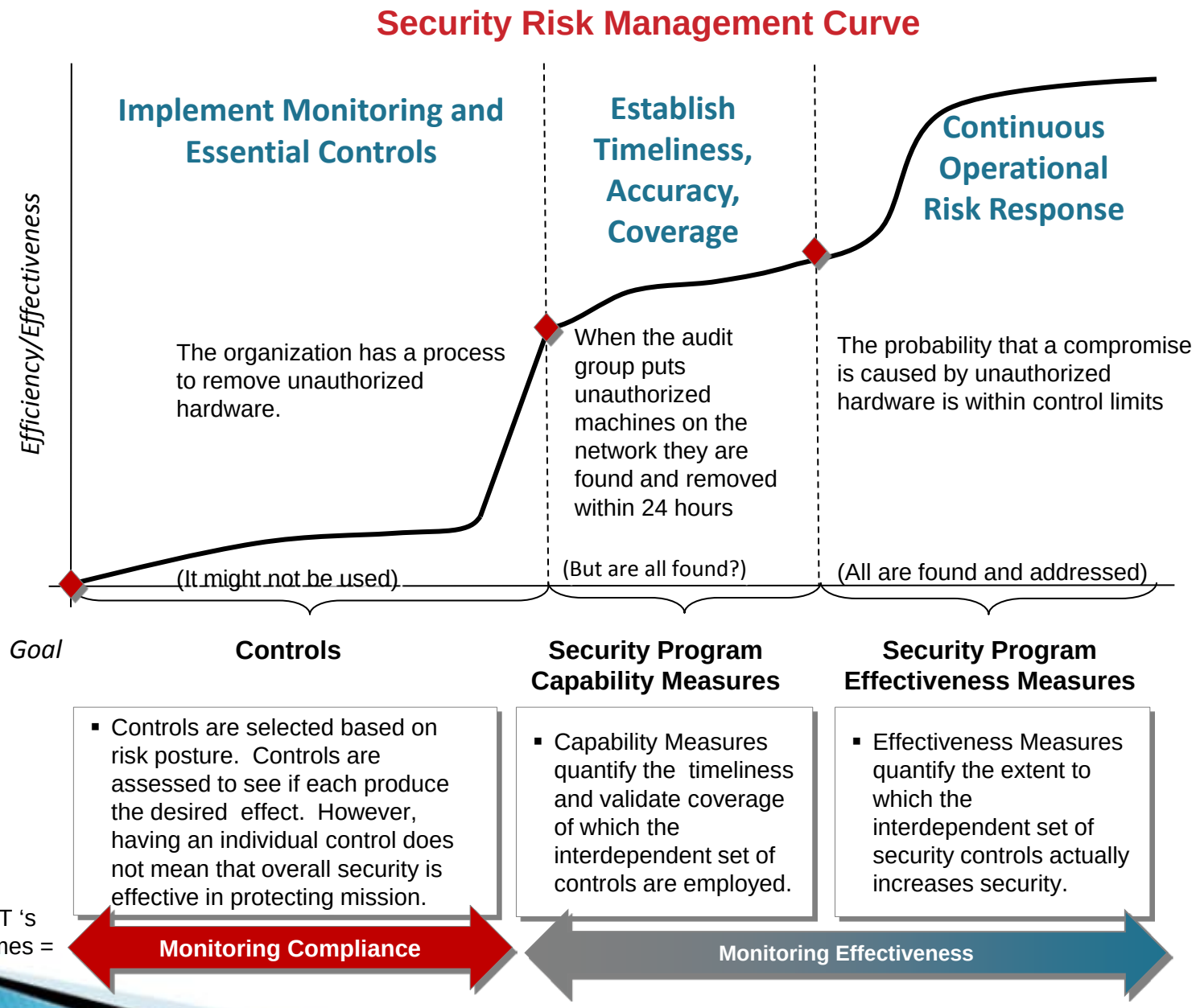


Risk Management

In a risk management model, grouped security activities are organized based on management and functional processes (i.e., operational and technical) and how they support the organization's risk to its mission

MBL TECHNOLOGIES

The community is moving towards an understanding that effectiveness of risk response is more valuable than compliance

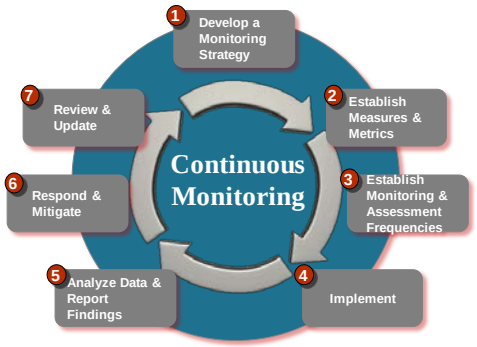


LINCOLN LABORATORY
MASSACHUSETTS INSTITUTE OF TECHNOLOGY

MBL TECHNOLOGIES

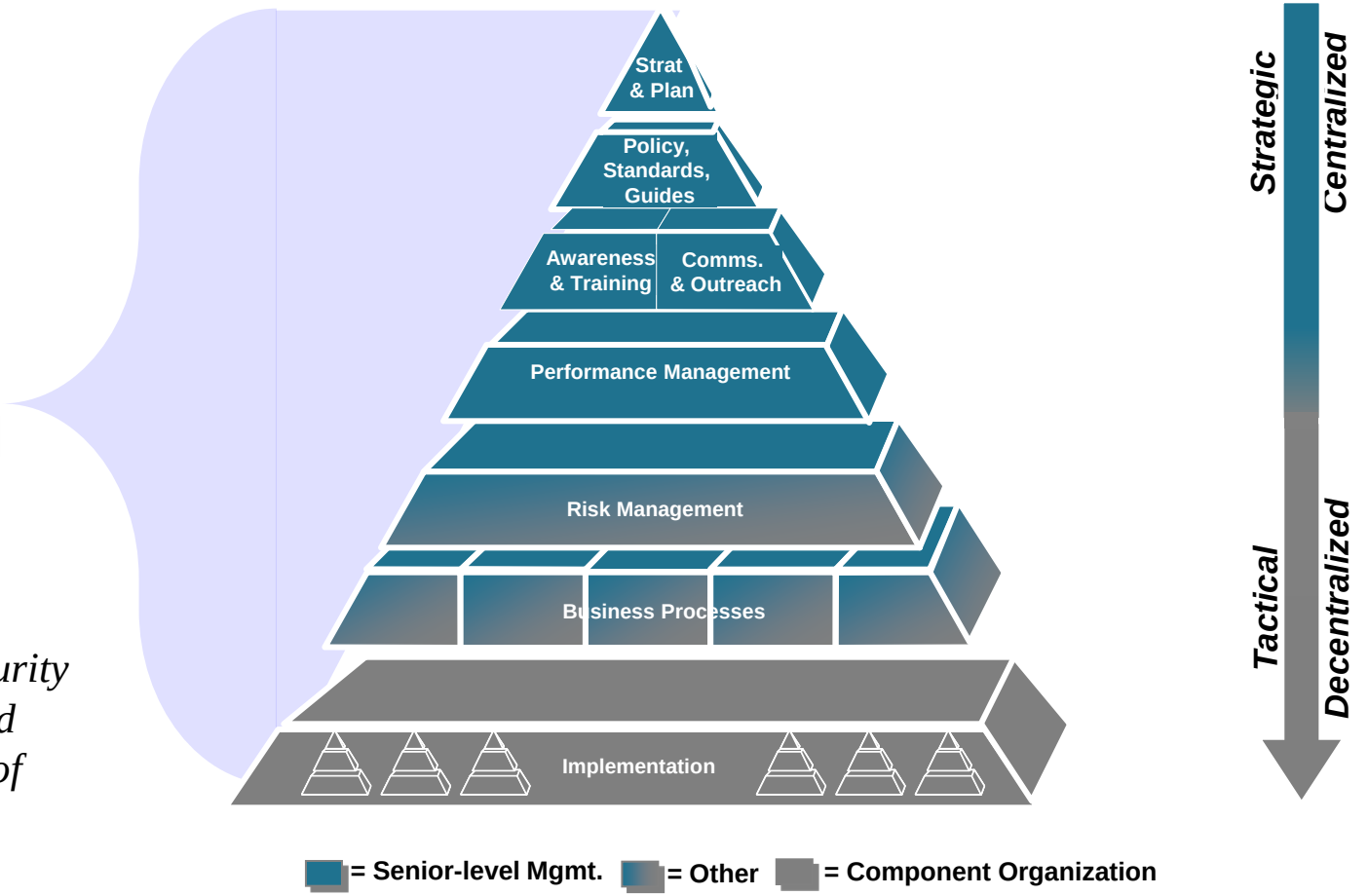
The risk management framework has become the dominant model to follow for the Federal government community

Continuous Monitoring



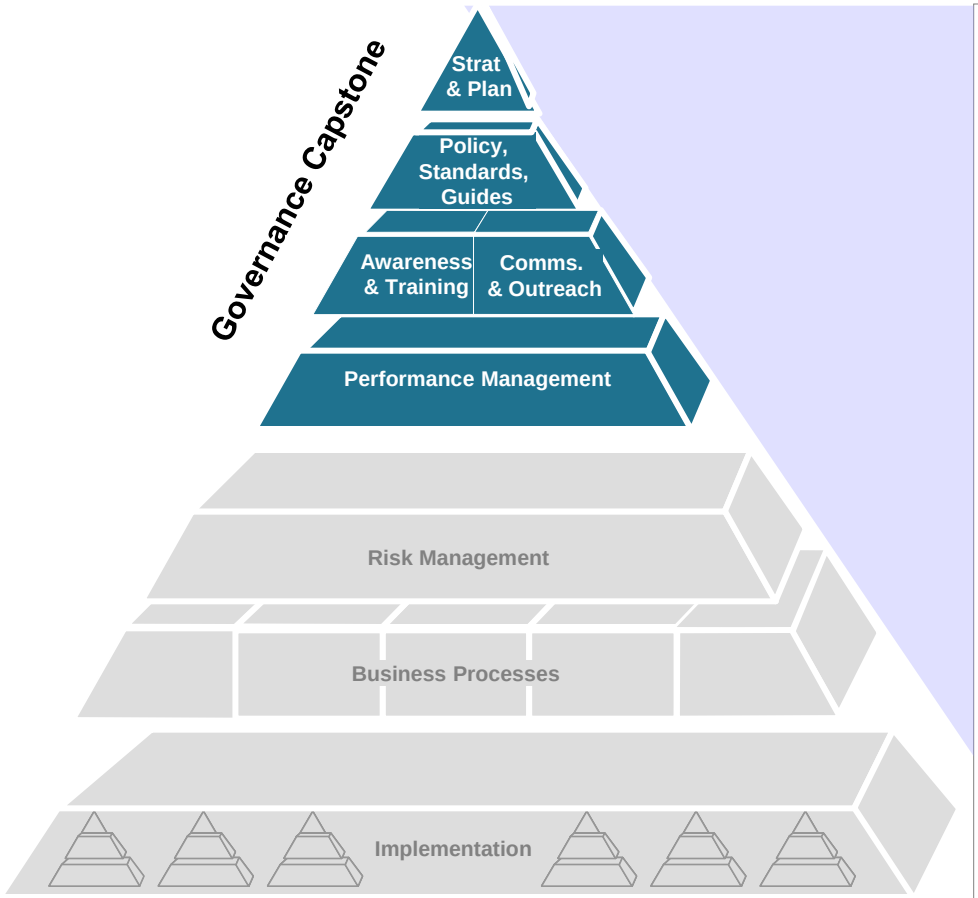
Recent NIST SP 800-39 guidance suggests that security testing should be prioritized based on the effectiveness of risk response

Risk Management Governance Framework



MBL TECHNOLOGIES

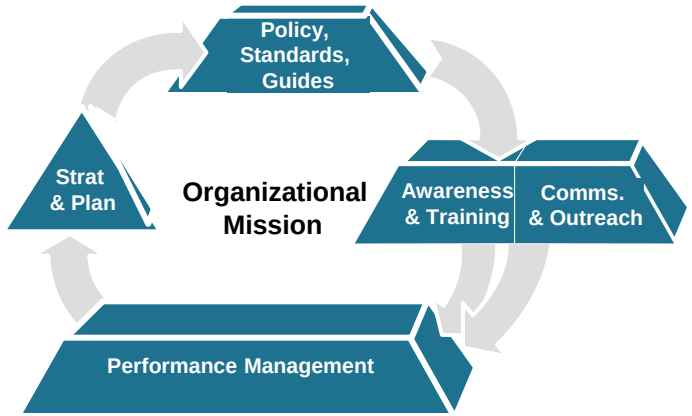
The capstone of the framework is a governance economy that should be the foundation of a strong continuous monitoring program



Governance Capstone

Continuous Monitoring Strategic Considerations

These components need to be considered in a holistic perspective relative to continuous monitoring…

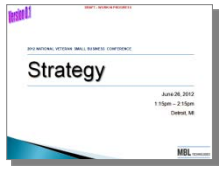


…to create a systematic economy ensuring that we are not stove-piping components of governance (and continuous monitoring) but rather taking an integrated approach to manage risk…

MBL TECHNOLOGIES

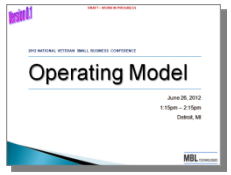
The seminal piece to an effective governance and continuous monitoring program is strategy and planning

Strategy and Planning



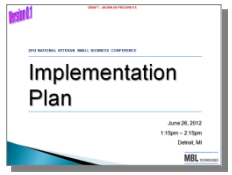
Strategy

Establishes continuous monitoring program vision, goals, and objectives



Operating Model

Establishes processes, organizational structure, stakeholder interaction model, and program enablers



Implementation Plans

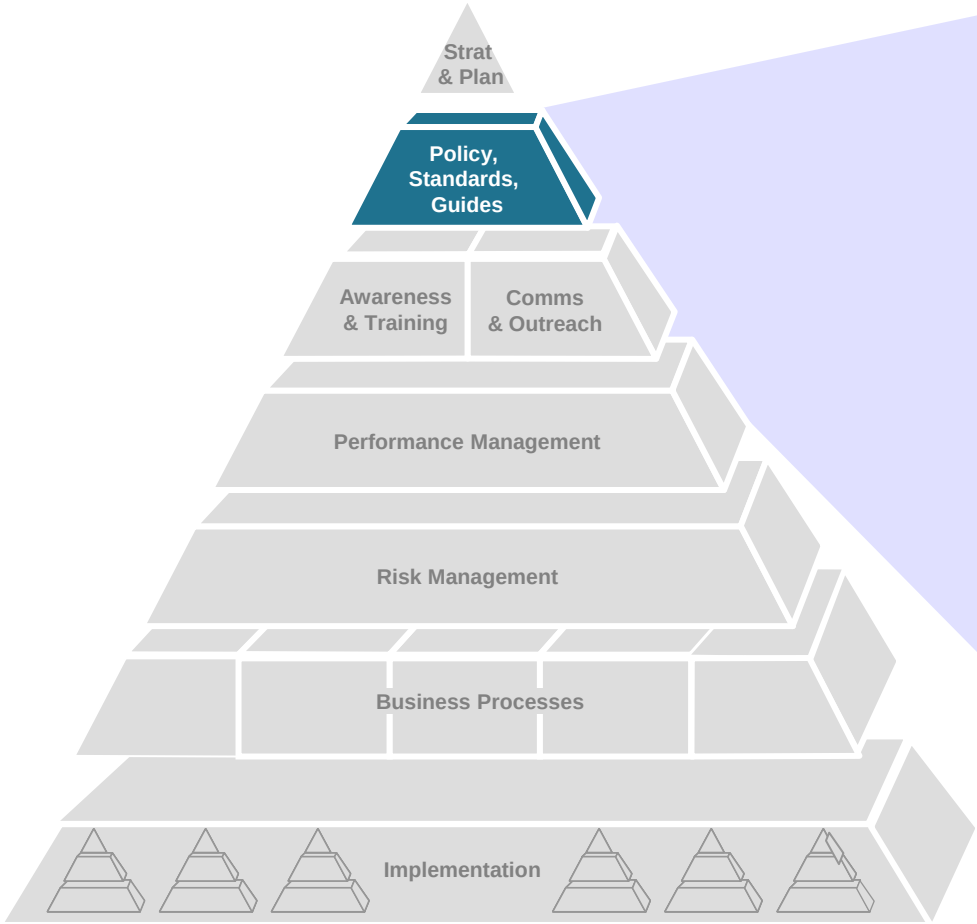
Detailed road maps with budgets resource allocation

Strategic Considerations

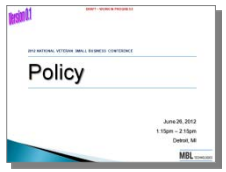
- Alignment with agency/corporate risk tolerance/threshold(s)
- Conformant with other existing IT strategy initiatives currently in place
- Buy-in with senior leadership/stakeholders (laying out incentives to address security)
- Resource allocation/constraints

MBL TECHNOLOGIES

Policy and Standards then provide the supporting "rules" and "how-to" to implement the continuous monitoring program



Policy and Standards

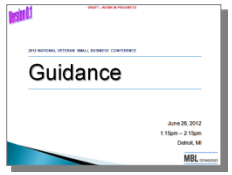


Policy

Establishes structured direction for organization's continuous monitoring program and roles/responsibilities

Standards

Provides control processes necessary to meet the requirements of the continuous monitoring policy statements



Guidance

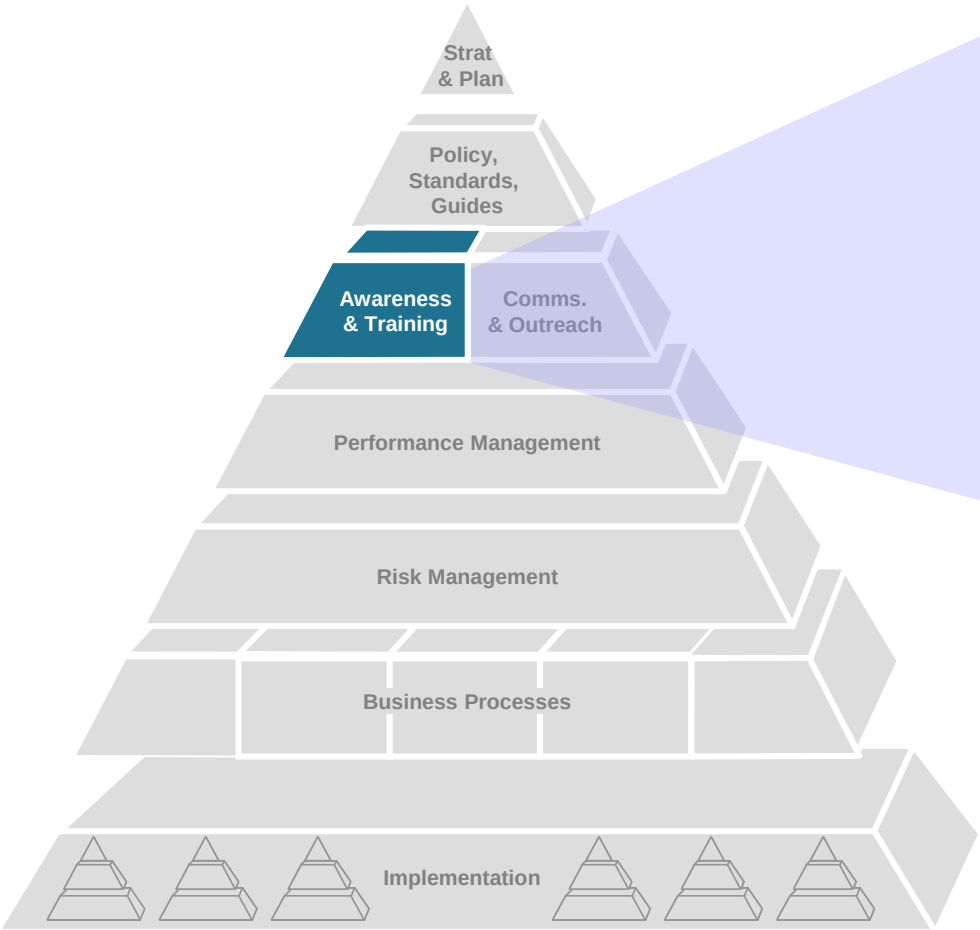
Detailed instructions on how to effectively implement control processes (the "how to")

Strategic Considerations

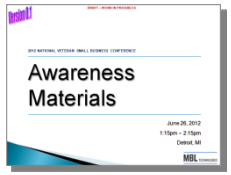
- Risk based flexibility and defined risk thresholds
- Established nomenclature/framework
- Life-cycle process flow to support policy development and maintenance relative to continuous monitoring
- Importance of consistency (Strategy – Policy)

MBL TECHNOLOGIES

Awareness and Training follows in providing for an interactive mechanism to achieve knowledge transfer across various roles



Awareness and Training



Awareness Materials

Communicate key continuous monitoring concepts, risks, principles through focused modalities

Training

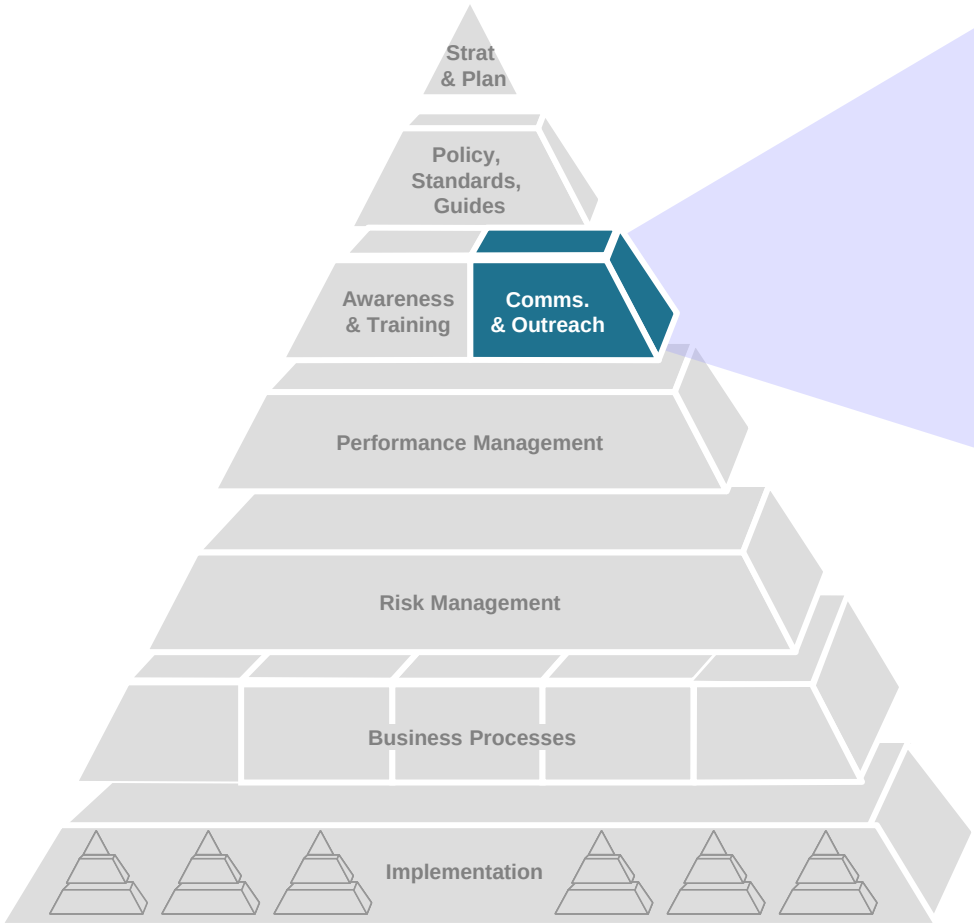
Provide role based instruction for staff with continuous monitoring responsibilities and processes

Strategic Considerations

- Tailored for applicable continuous monitoring roles (role based training)
- Recognition of different modalities and mechanisms
- Extension of strategic priorities (e.g., embed continuous monitoring with other information security topics (e.g., FISMA))

MBL TECHNOLOGIES

Communication and Outreach is the means by which program concepts are exchanged to increase understanding and integration



Communications and Outreach

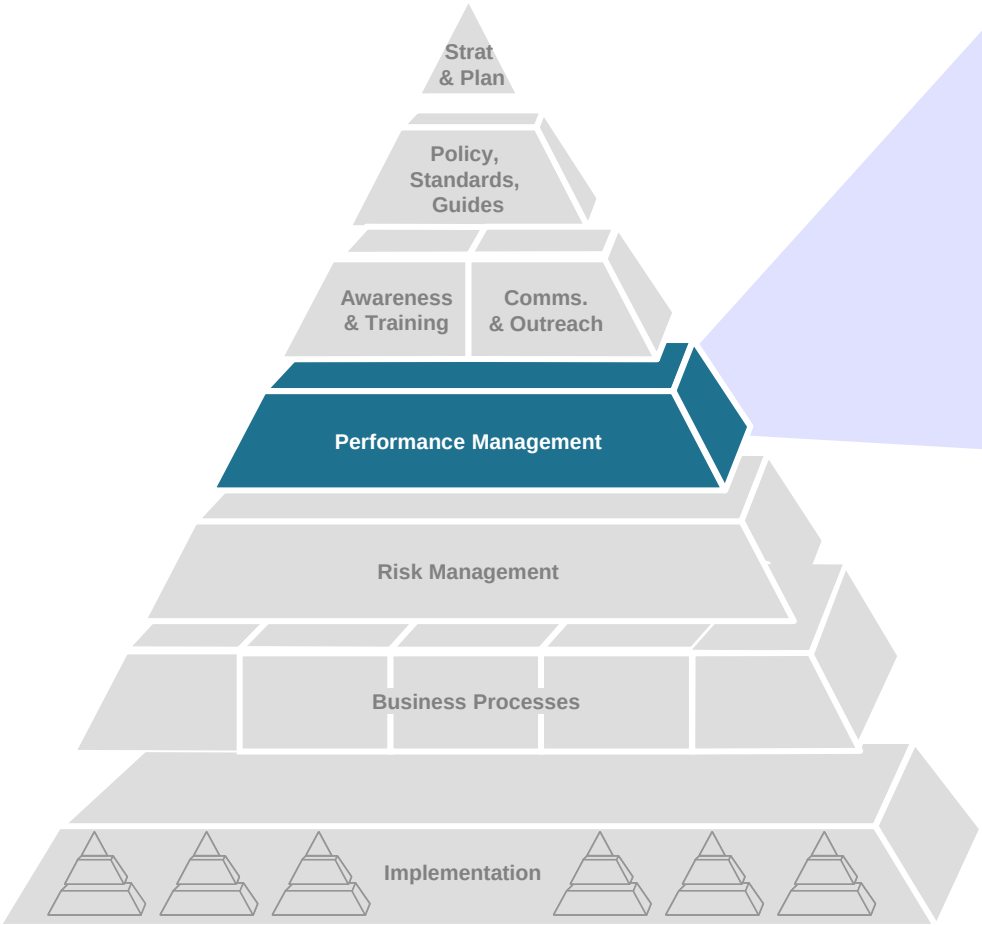
Push Communications
Continuous monitoring program information is sent to stakeholders via work shops, one-on-one meetings, website, e-mail, etc.

Pull Communications
Continuous monitoring programmatic Information is gathered via feedback, input surveys, focus groups, other automated mechanisms

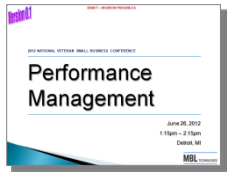
Strategic Considerations

- Consistency/modality of messaging
- Applicability of internal and external stakeholders
- Effective definition and understanding of relationships – understanding of audience
- Conduit to trending – internally and externally
- Influences the structure of the continuous monitoring scoring dashboard

Performance Management provides the key mechanism for ensuring that the defined continuous monitoring metrics are tracked



Performance Management



Performance Management

Measure and report on organization's adherence to agreed upon continuous monitoring metrics (e.g):

- **Assets Management** (based on common platform enumeration (CPE) to capture asset type)
- **Vulnerability Management** (based on Common Vulnerability Scoring System (CVSS) ratings)
- **Common Configuration Enumeration**(based on adherence to the United States Governance Configuration Board (USGCB) and the Federal Desktop Configuration Compliance (FDCC) baselines

Strategic Considerations

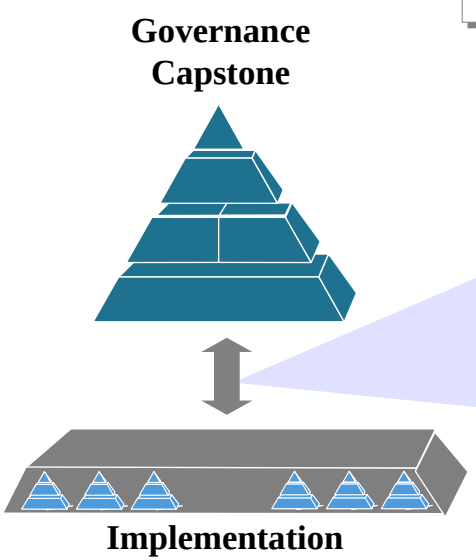
- Enabler for effective decision-making based on risk
- Proactive versus reactive compliance
- Balance of individual versus meta analysis
- Industry benchmarking (e.g., Federal Continuous Monitoring Working Group) should drive thresholds
- Definition of effectiveness measures

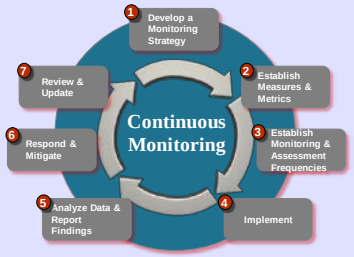
MBL TECHNOLOGIES

Agreement on risk thresholds and a tolerance level among component organizations is critical to the success of the program

Risk Management (and Supporting Business Processes)

What is needed	How is it influenced
Coordinated risk thresholds	Agency-level working group(s)
Uniform oversight and evaluation	Continuous monitoring strategy
Prioritized risk mitigation (based on threat/vulnerabilities)	Selection of Agency monitoring tool(s)
	Consensus on scoring metrics

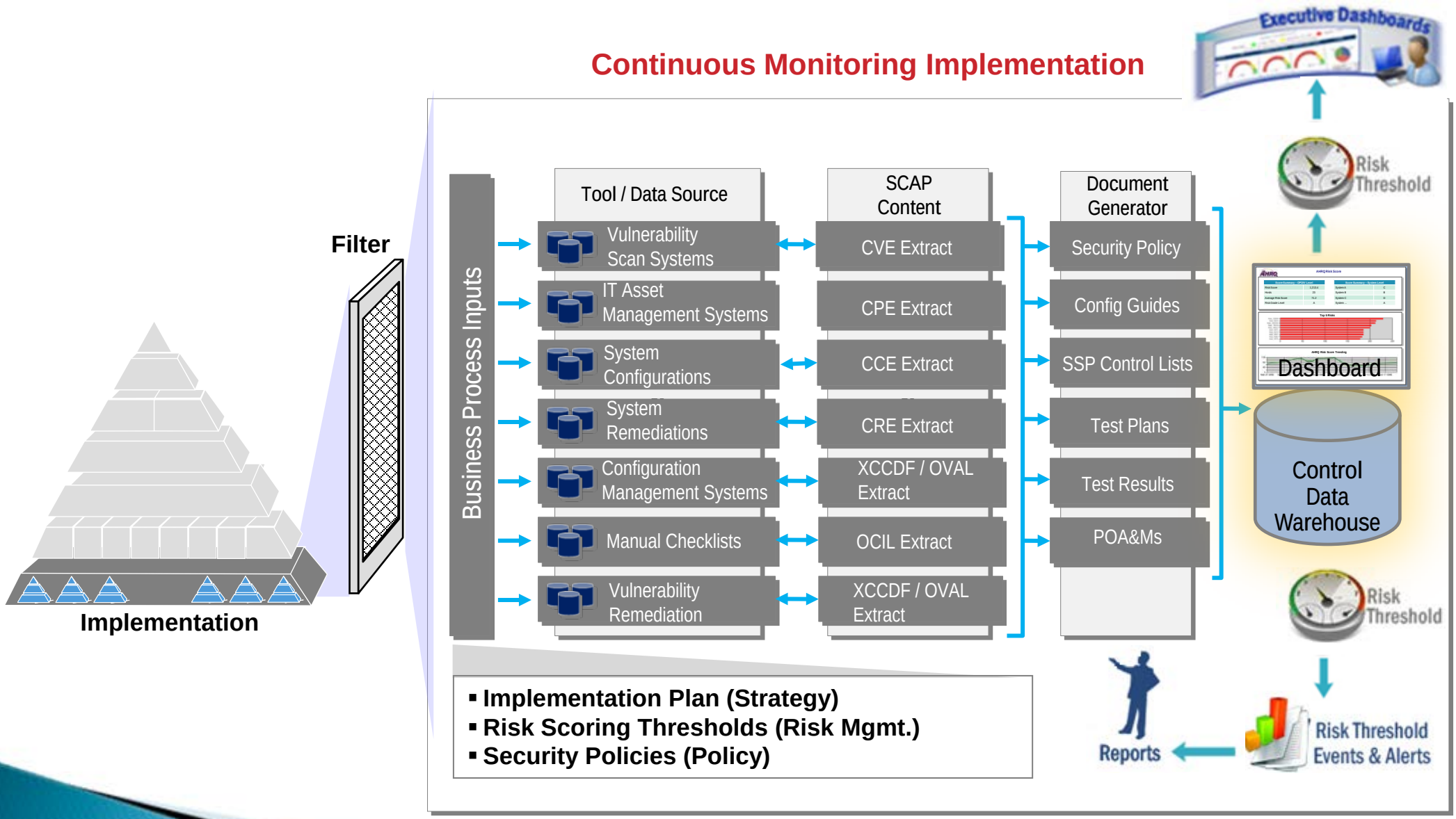




What is needed	How is it influenced
Strong understanding of asset inventory (that support business)	Maturity of services, business, and supporting tools
Defined and consistent metrics	Consensus on scoring metrics
Centralized tools and monitoring	Incentivizing behavior change through scoring
Mature SCAP content	

MBL TECHNOLOGIES

From a continuous monitoring implementation perspective, several key considerations must be factored into the design of the model



MBL TECHNOLOGIES

Questions…

Contact Information

MBL TECHNOLOGIES
Move. Build. Lead

Jamie Miller, MBA, PMP
Senior Manager

1 Research Court, Suite 450
Rockville, MD 20850

Cell: 202-390-8919
Fax: 240-399-4215
jamie.miller@mbltechnologies.com
jamie.miller@hhs.gov

For more information about **MBL Technologies**, please visit us at:

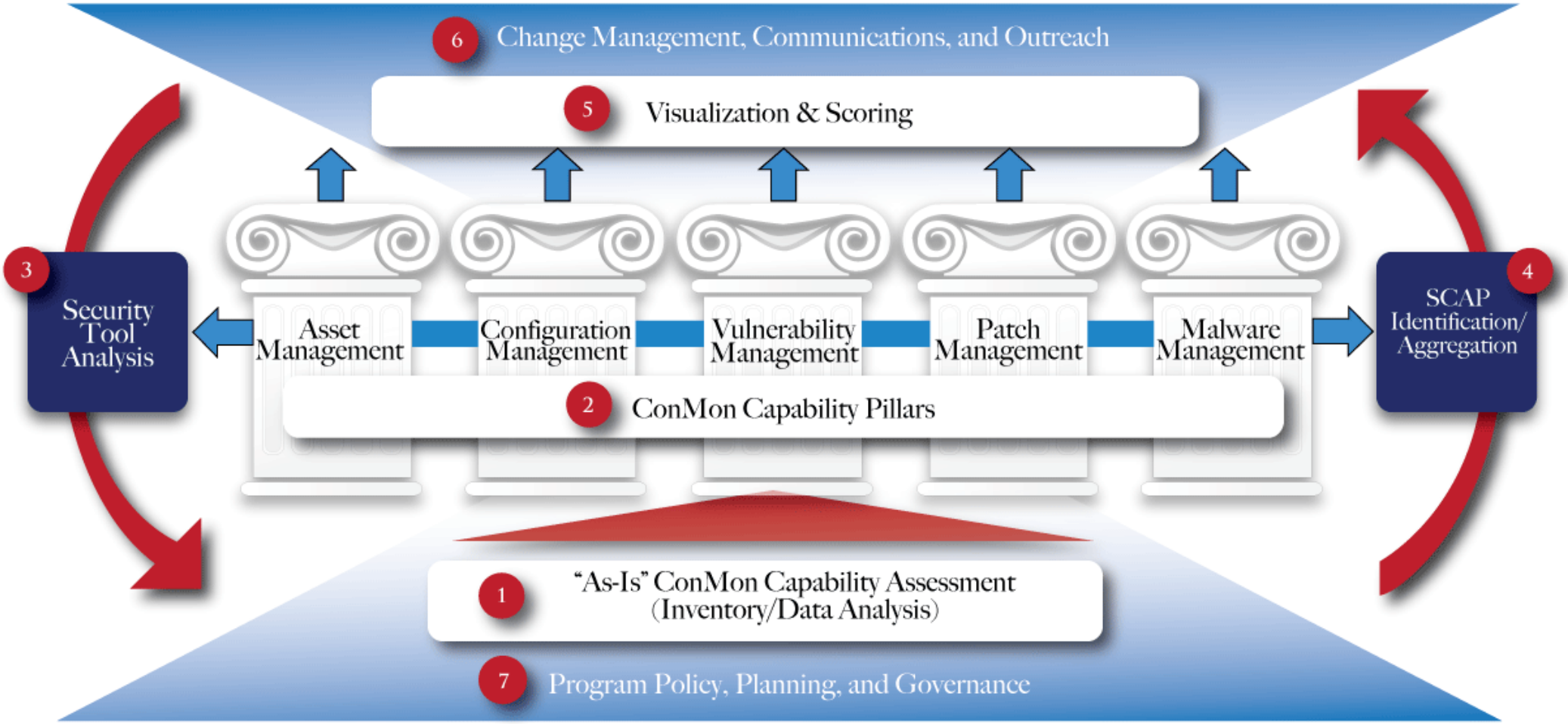
http://www.mbltechnologies.com …Or on LinkedIn –
and Facebook –

MBL TECHNOLOGIES

SUPPLEMENTAL SLIDES

MBL TECHNOLOGIES

CONTINUOUS MONITORING SERVICE OFFERING



MBL TECHNOLOGIES