Making Security Measurable and Manageable

- Author:
  - Robert A. Martin, *The MITRE Corporation*.
- Conference:
  - 2008 IEEE Military Communications Conference (MILCOM 2008).
- Journal:
  - The Journal of Defense Software Engineering, September/October 2009, pp.26-32.
- White Paper:
  - Department of Homeland Security (DHS), 2010.

Outline

- Introduction
- Architecting Security
- Building Blocks for Architecting Measurable Security
- How the Architectural Building Blocks Come Together
- Conclusions

Introduction (1/3)

- The security, integrity, and resiliency of information systems is a critical issue for most organizations.
- One popular approach is the use of standard knowledge representations, enumerations, exchange formats and languages, and a sharing of standard approaches to key compliance and conformance mandates.
- These "*Making Security Measurable*" (MSM) initiatives provide the foundation for answering today's increased demands for accountability, efficiency, resiliency, and interoperability without artificially constraining an organization's solution options.

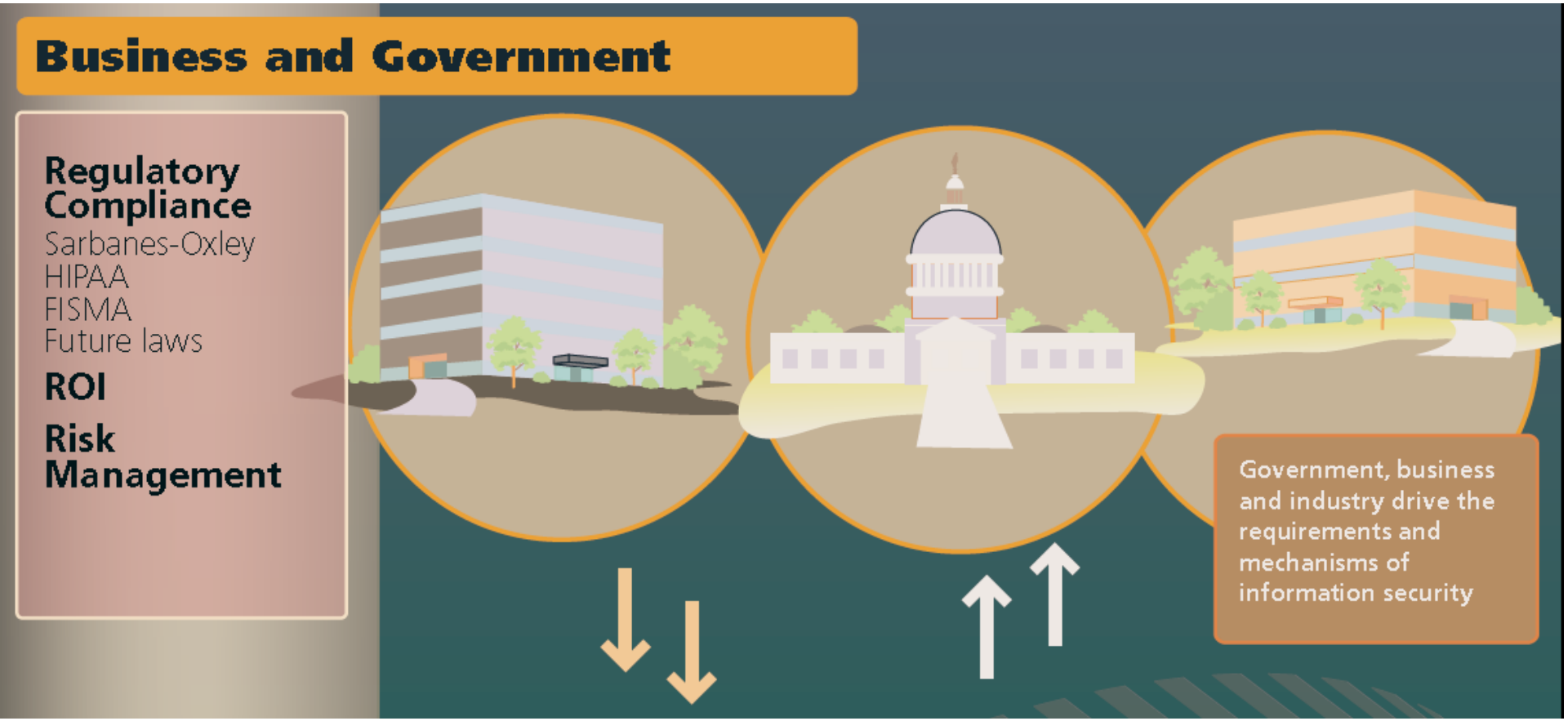
Introduction (2/3)

- This article explores how these standards are facilitating the use of automation to assess, manage, and improve the security posture of enterprise security information infrastructures while also fostering resiliency and effective security process coordination across the adopting organizations.
- To make the finding and reporting issues consistent and composable across different tools, there has to be a set of standard definitions of the things that are being examined, reported, and managed by those different tools.
- Information security measurement and management as currently practiced is complex, expensive, and fraught with unique activities and tailored approaches.

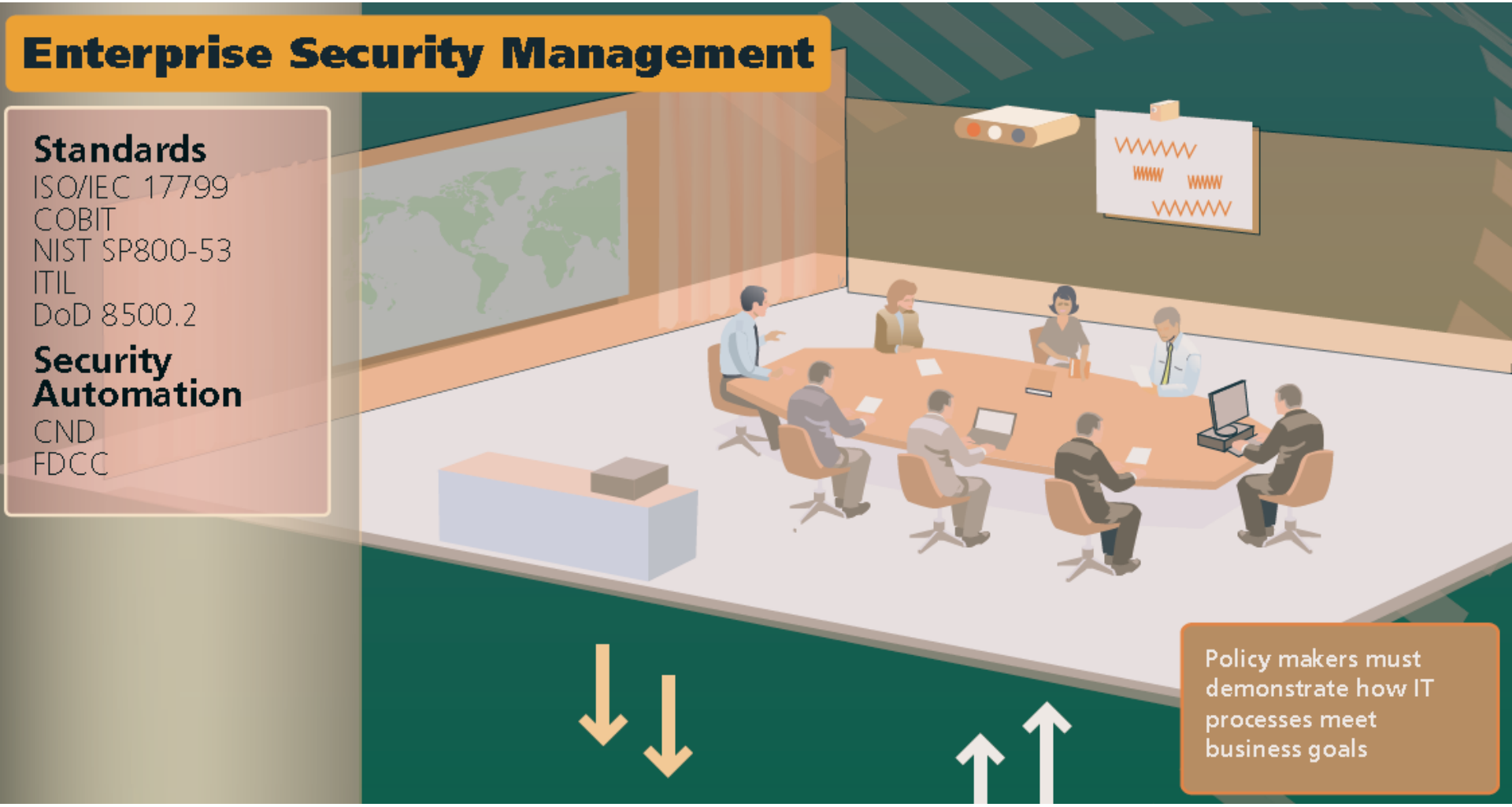
Introduction (3/3)

- Solving the variety of challenges currently facing enterprises with regards to incident and threat management, patching, application security, and compliance management requires fundamental changes in the way vendor technologies are adopted and integrated.
- The strategy must be neutral to the specific solution providers while also being flexible enough to work with several different solutions simultaneously.
- The new approach should enable the elimination of duplicative and manual activities as well as improve both the resiliency and organizational ability to leverage outside resources and collaborate with other organizations facing the same threats and risks.

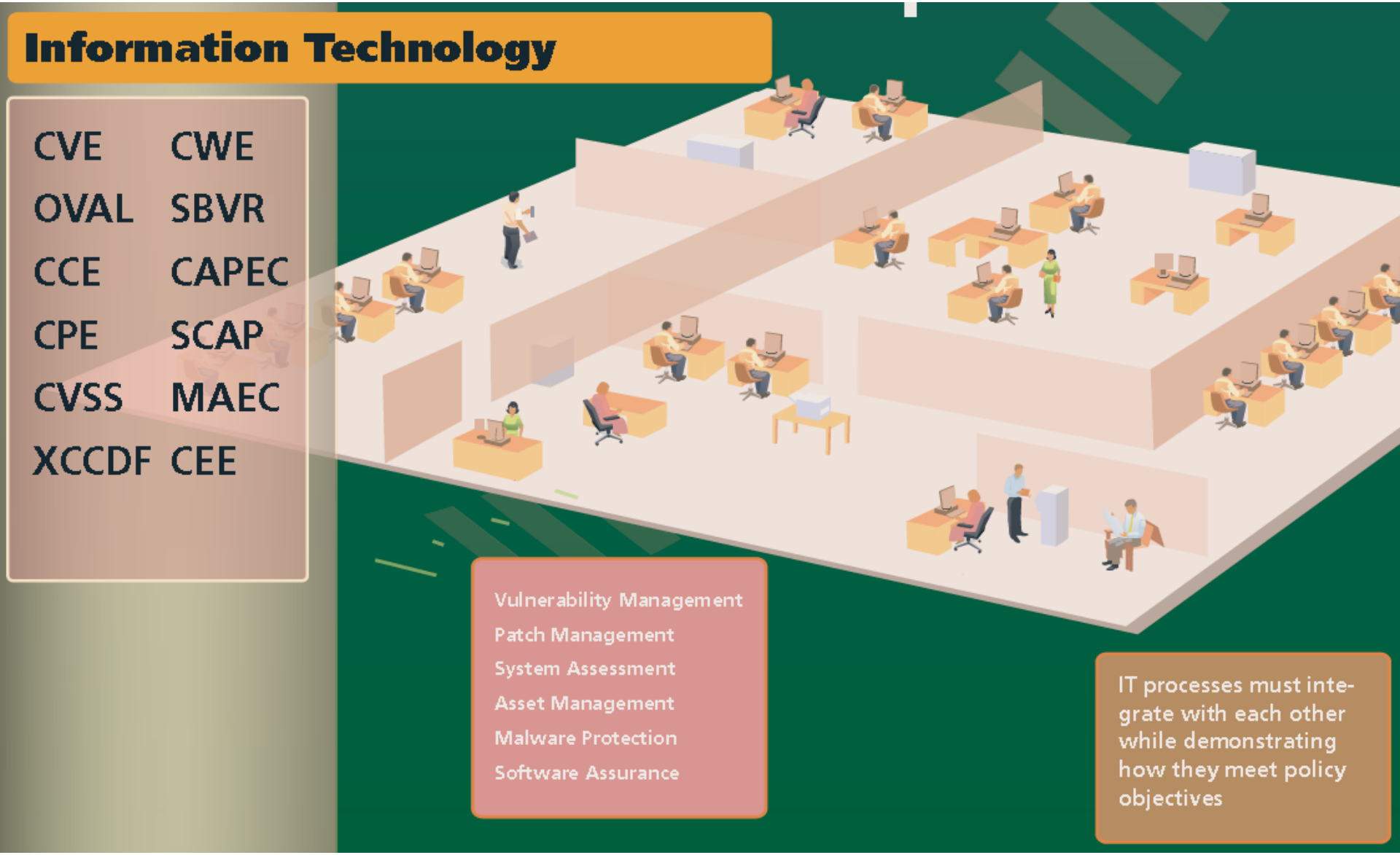
Benefits of Making Security Measurable illustration (1/3)



Benefits of Making Security Measurable illustration (2/3)



Benefits of Making Security Measurable illustration (3/3)



Architecting Security

- Both the U.S. government and commercial enterprises are already starting to deploy new approaches to security measurement and management that leverage interoperability standards and enable enterprise-wide security measurement and policy compliance efforts.
- These security architecture-driven measurement and management standards are already providing ways for these organizations to create test rules about their minimum secure configurations, mandatory patches, and unacceptable coding practices that can be assessed, reported, and any subsequent remediation steps planned, executed, and confirmed using commercial tools.
- These standards also provide a basis for repeatable, trainable processes and sharing along with enabling automation-based testing methods for deployment validation and regression testing throughout the operational lifetime of the systems.

Building Blocks for Architecting Measurable Security

- **4 basic building blocks for architecting measurable security:**
  - Standardized **enumerations** of the common concepts that need to be shared.
  - **Languages** for encoding high-fidelity information about how to find the common concepts and communicating that information from one human to another human, from a human to a tool, from one tool to another tool, and from a tool to a human.
  - Sharing the information through content **repositories** in languages for use in broad communities or individual organizations in a way that minimizes loss of meaning when content is being exchanged between tools, people, or both.
  - **Uniformity of adoption** achieved through branding and vetting programs to encourage the tools, interactions, and content remain standardized and conformant.

Enumerations

- Enumerations catalog the fundamental entities and concepts in information assurance, cybersecurity, and software assurance that need to be shared across the different disciplines and functions of these practices.

Enumerations

Name	Topic
CVE	Standard identifiers for publicly known vulnerabilities.
Common Weakness Enumeration (CWE)	Standard identifiers for the software weakness types in architecture, design, or implementation that lead to vulnerabilities.
Common Attack Pattern Enumeration and Classification (CAPEC)	Standard identifiers for attacks.
Common Configuration Enumeration (CCE)	Standard identifiers for configuration issues.
Common Platform Enumeration (CPE)	Standard identifiers for platforms, operating systems, and application packages.
The SANS Institute Top 20 Security Risks	Consensus list of the most critical vulnerabilites that require immediate remediation.
Open Web Application Security Project's Top 10	List of the 10 most critical Web application security flaws.
Web Application Security Consortium's Threat Classification	List of Web security attack classes.
CWE/SANS Top 25 Most Dangerous Programming Errors	Consensus list of the most dangerous types of programming errors that require immediate attention.

CVE: Common Vulnerabilities and Exposures

Languages

- Standardized **languages** and **formats** allow uniform encoding of the enumerated concepts and other high-fidelity information for communication from human to human, human to tool, tool to tool, and tool to human.

Languages

Name	Topic
XCCDF	An XML specification language for writing security checklists, benchmarks, and related documents.
OVAL	An XML state expression language for writing assessment tests about the current state of an asset and expressing the results.
Common Vulnerability Scoring System (CVSS)	A method for conveying vulnerability-related risk and risk measurements.
Common Result Format (CRF)	A standardized IT asset assesment result format that facilitates the exchange and aggregation of assessment results.
Semantics of Business Vocabulary and Business Rules (SBVR)	A vocabulary and rules for documenting the semantics of an area of a business' vocabulary, facts, and processes.
Common Event Expression (CEE)	A language and syntax for describing computer events, how the events are logged, and how they are exchanged.
Malware Attribute Enumeration and Characterization (MAEC)	A language for decribing malware in terms of its attack patterns, detritus, and actions.
Common Announcement Interchange Format (CAIF)	An XML-based format for storing and exchanging security announcements.

XCCDF: Extensible Configuration Checklist Description Format

OVAL: Open Vulnerability and Assessment Language

Repositories

- Repositories allow common, standardized content to be used and shared, whether across broad communities or within individual organizations.
- The sharing of content has been done for some time but doing so in standard machine-consumable languages and formats using standard enumerated concepts is fairly recent.
- There are also closed repositories where, for instance, a company may write a tailored set of policies about what they want to do to comply with the Sarbanes-Oxley Act.

Repositories

- They don’t necessarily want to share with the world, but they want to be standard across all of the different elements of their company and they want it available for their auditors and possibly their partners.

Repositories

Name	Topic
DoD Computer Emergency Response Team (CERT)	Information Assurance Vulnerability Alerts (IAVAs) and Defense Information Systems Agency's (DISA) Security Technical Implementation Guides (STIGS)
The Center for Internet Security (CIS)	CIS Security Configuration Benchmarks
National Security Agency (NSA)	NSA Security Guides
National Vulnerability Database (NVD)	US-CERT advisories, US-CERT Vuln Notes, CVE and CCE Vulnerabilities, checklists, OVAL definitions, and U.S. Information Security Automation Program (ISAP) and Security Content Automation Protocol (SCAP) content.
Red Hat Repository	OVAL Patch Definitions for Red Hat Errata security advisories
OVAL Repository	OVAL Vulnerability, compliance, inventory, and patch definitions.

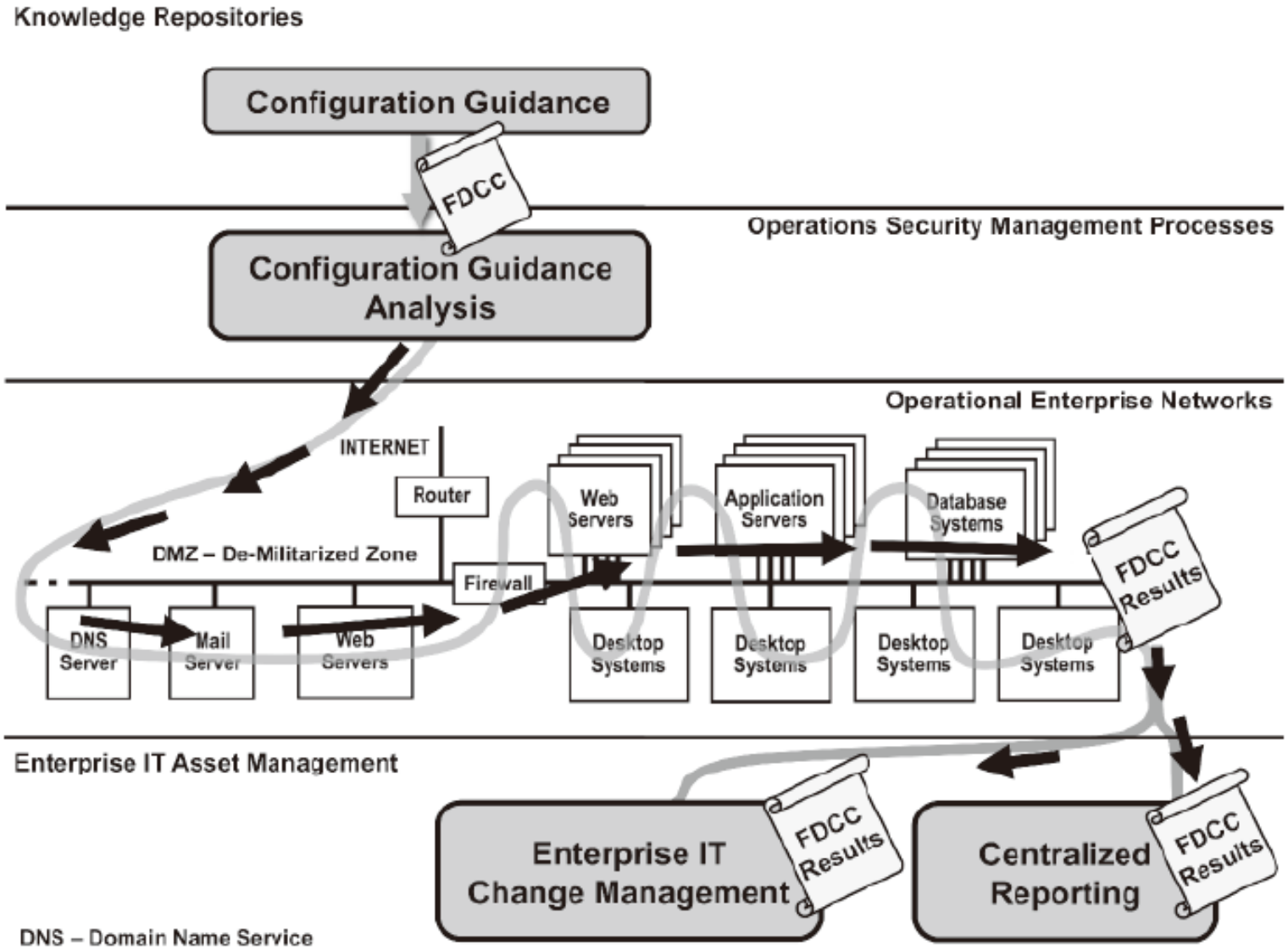
Uniformity of Adoption

- Uniform adoption of standards by the community is best achieved through branding/vetting programs that can help the tools, interactions, and content remain conformant with the accepted standards.
- Information security products and services can interoperate with other compatible products that each have correctly mapped their capabilities concept of a particular vulnerability to the correct CVE (Common Vulnerabilities and Exposures) Identifier for that vulnerability.
- The National Institute of Standards and Technology (NIST) has also initiated a Security Automation Validation Program (Security Content Automation Protocol, SCAP) for those vendors that currently provide (or intend to provide) SCAP-validated tools.

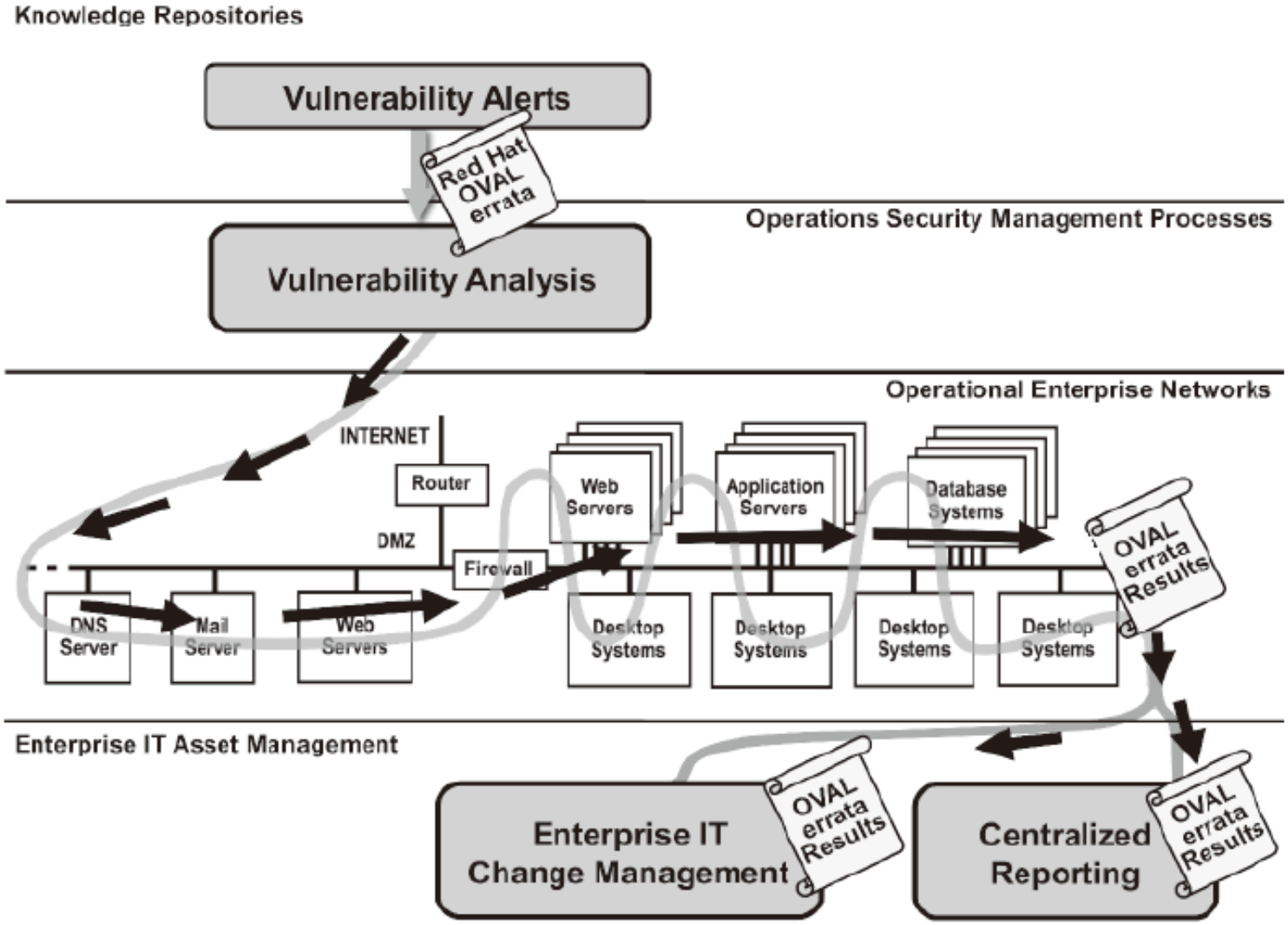
How the Architectural Building Blocks Come Together

- The building blocks of architecting for measurable security are already in use in the enterprise security areas of configuration compliance assessment, vulnerability assessment, system assessment, and threat assessment.
- An Office of Management and Budget (OMB) memorandum references the content in NIST's National Vulnerability Database (NVD).
- This guidance is also referred to as part of the Federal Desktop Core Configuration (FDCC) and is intended to bring consistency in the specific secure system software configuration of Microsoft Windows XP and Vista in use by the federal government.
- China: CGDCC (Chinese Government Desktop Core Configuration)

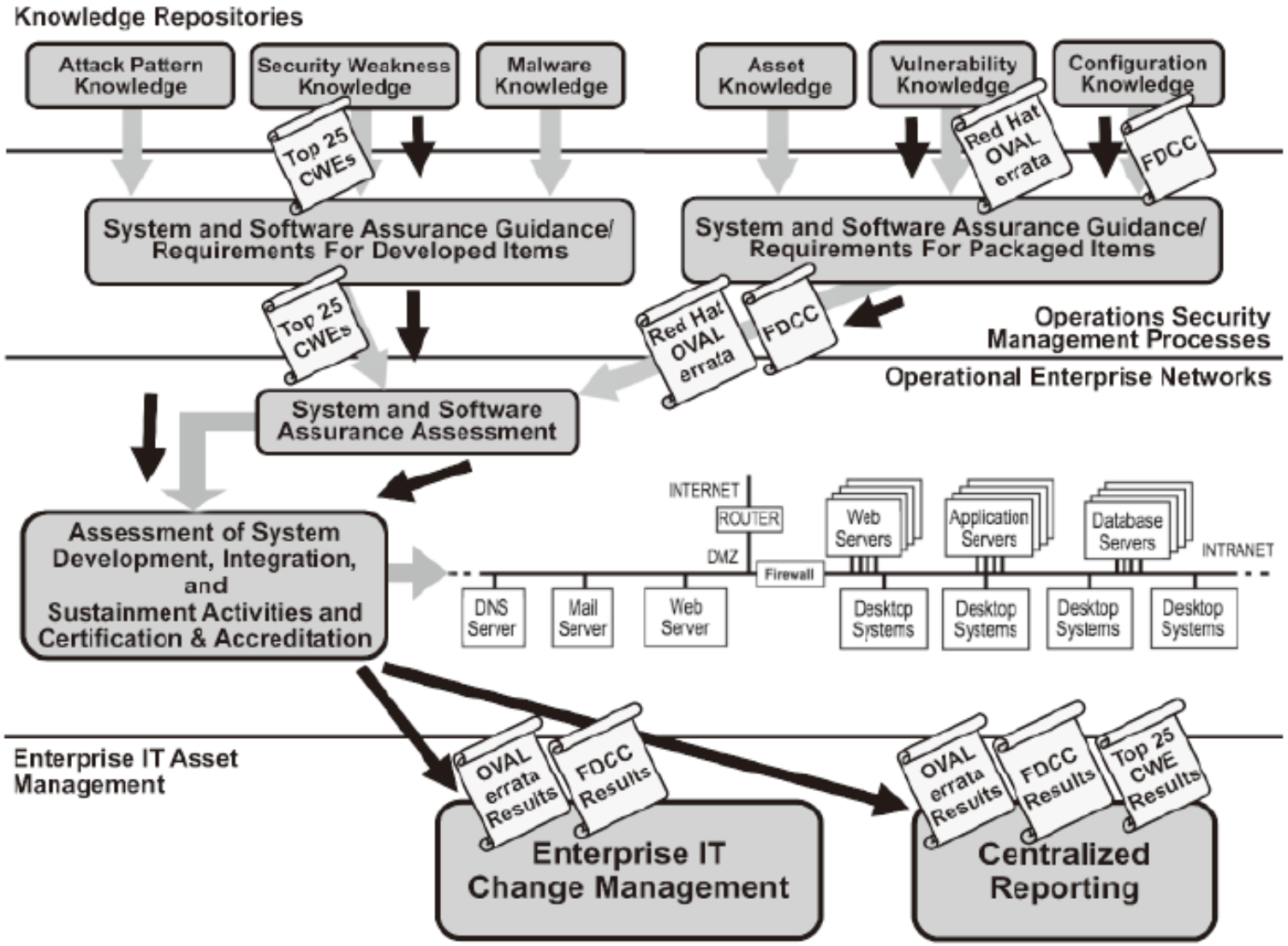
Assessment of Configuration Compliance Using Standards Vulnerability Assessment



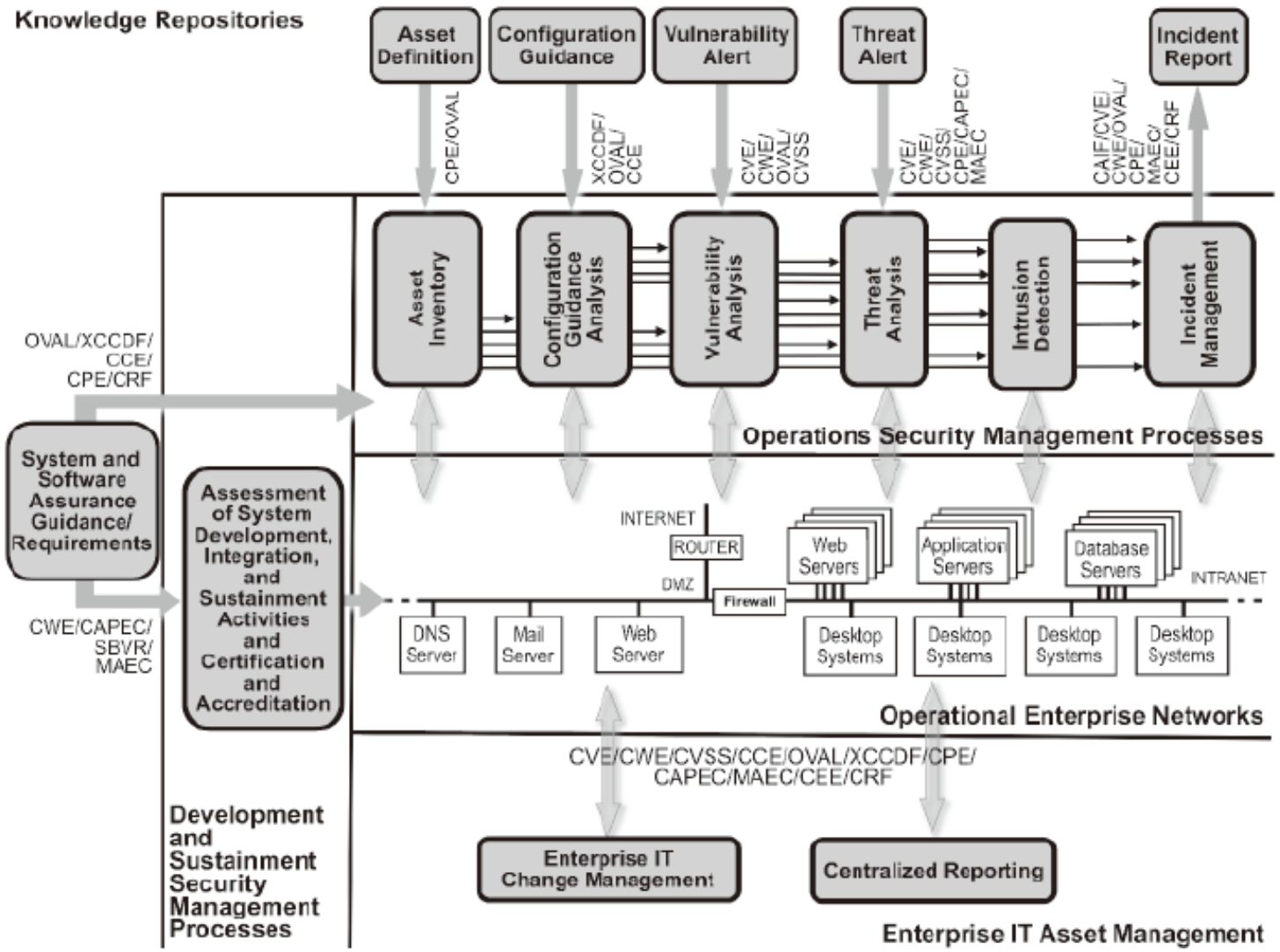
Assessment of Vulnerability Remediation Status



System Certification and Accreditation



Cyber Security Measurement and Management Architecture



How Data Standards Provide for Measurable and Manageable Security

- The measurability and manageability of security is improved through enumerating baseline security data, using standardized languages as means for accurately communicating the information, and sharing that information with users in repositories.

Vulnerability Management

CVE – standardized identifiers for vulnerabilities
CVSS - scores vulnerability severity
OVAL - standardized tests for the presence of vulnerabilities

Configuration Management

OVAL - tests for the presence of vulnerabilities, configurations, assets
CCE - standardized identifiers for configuration controls

Compliance Management

OVAL - tests for the presence of configurations and assets
XCCDF - language to express configuration guidance

Asset Management

CPE - standardized identifiers for platforms and configuration controls
OVAL - tests for the presence of assets

Malware Management

MAEC – malware attribution
OVAL - tests for the presence of vulnerabilities, configurations, patches, assets

System Assessment

CVE – standardized identifiers for vulnerabilities
CCE - standardized identifies for configuration controls
CPE - standardized identifiers for platforms and configuration controls
OVAL - tests for the presence of vulnerabilities, configurations, patches, assets

Threat Analysis

CVE – standardized identifiers for vulnerabilities
CWE – standardized identifiers for software weakness types
CAPEC - standardized identifiers for attack patterns
CPE - standardized identifiers for platforms and configuration controls

Application Security

CWE – standardized identifiers for software weakness types
CVE – standardized identifiers for vulnerabilities
OVAL - standardized tests for the presence of vulnerabilities

Incident Management

CVE – standardized identifiers for vulnerabilities
CVSS - scores vulnerability severity
OVAL - standardized tests for the presence of vulnerabilities, configurations, patches, assets

Reusable and Shared Repositories

- These same standards can be used to capture how an organization has configured and set up a new system when it has been approved for use in an enterprise.
- By using these standards, this information can go right into operational network management so that an organization can make sure the new system continues to be configured in the way that it was approved.

Conclusions

- The use of architecture and systems engineering principles has been shown to be effective and enabling.
- Ongoing efforts to address and evolve all of the activities in this arena will greatly benefit from the continued application of this methodology.
- This article has outlined the changes in security practices and technologies and has shown specific and measurable changes that are directly related to the use of architectural methods on security of information technologies in government and private industry.