Information Security Management Beyond Certification and Accreditation

Vijay Rachamadugu, CISSP
The MITRE Corporation
7515 Colshire Drive
McLean, VA 22102 USA
vijayr@mitre.org

John A. Anderson
Cougaar Software, Inc.
1945 Old Gallows Road, Suite 100
Vienna, VA 22182 USA
janderson@cougaarsoftware.com

ABSTRACT

Traditional information security approaches rely too heavily on system certification and accreditation (C&A) to ensure that a system is sufficiently secure. Such approaches inadequately address security during acquisition and/or development, which increases the risk of the system containing inherent computer vulnerabilities and exposures that may lead to inappropriate issuance of an Authority to Operate (ATO) as a result of unintentional oversight of problems or pressure to deploy despite recognized residual risks. In certain instances, testing by an independent authority may mitigate some of the risks; however, such testing is often undertaken near the end of the development/acquisition cycle. This paper describes proven elements of a more comprehensive methodology that addresses information security throughout the acquisition and system life cycle from both a system and enterprise perspective. The paper applies the authors' research on Roadmap for Information Security Guidance for Enterprise Transformation to information security management in development and acquisition. The content and references can be used for organizations striving to improve their acquisition, system development and security management processes.

KEY WORDS

Information Security, Enterprise Architecture, Certification, Accreditation, Security Management

1 THE SECURITY CHALLENGE

There is a misconception that systems that have completed information security certification and accreditation (C&A) are sufficiently reliable and secure to operate within an enterprise's operational environment. Actually, C&A only ensures that systems and major applications have been reviewed, their vulnerabilities have been documented, and recommendations have been made as to whether they should be placed into operation. This paper describes elements of a comprehensive life cycle approach that manages information security throughout the entire software life cycle, from both a system and enterprise level—C&A is a distinct process applied within that approach. A more holistic approach to information security can reduce security risk as well as software development/maintenance costs.

All information systems operating on U.S. government networks must have a formal security review at least every three years as a requirement for compliance with the Federal Information Security Management Act (FISMA) of 2002. Unfortunately, information security is a goal and a process that are typically not sufficiently integrated into the overall business operations and/or enterprise solution acquisition process; information security is often delegated to information technology (IT) specialists at the end of the development process, which increases the cost of integrating adequate security mechanisms into the system.

In most cases, the guidance available from certification and accreditation policies and instructions is general. Targeted for the entire enterprise, it is not specific to the operational requirements of the system being developed, and its interpretation is left to the program manager. In certain instances, the guidance may be outdated and no longer applicable to a fast changing current environment. Hence, the implementation is dependent on the capabilities and knowledge of the development contractor. Since contractors and program managers are typically not security specialists, security requirements analysis is often deferred until later in the development process.

Such situations lead to discovery/exposure of the problems during Operational Test and Evaluation which much later in the acquisition life cycle. By that time, the system is so far in the development process that minimal choices exist for the correction and/or mitigation of the exposed vulnerabilities without substantial redesign.

2 ADDRESSING THE PROBLEM VIA A COMPREHENSIVE ENTERPRISE-BASED APPROACH

For systems engineering processes to effectively ensure adequate information security, Information security must be addressed from both a system-specific and an enterprise level. Each system acquisition or development effort must be evaluated individually to determine the particular information and processes to be protected and to determine appropriate measures for managing that protection. That system will operate within the context of the operations its supports, the organizations using the system, their missions, and their adversaries. This paper emphasizes the integration of information security engineering from both a systems and enterprise level throughout the system's life cycle. A plethora of information security challenges will continue to exist and emerge, thus the need for organizations to maintain a staff of security specialists that continuously maintain awareness of advances in cyber-security, both adversarial and preventative. However, all management and engineering staff need to maintain general understanding of information security concerns and approaches, and awareness of their specific role. Integrating the expertise and guidance of the information security team into the overall system acquisition and life cycle development system, and defining an enterprise-based comprehensive approach to information security is essential to effectively and efficiently assuring enterprise information security.

The U.S. federal government and the Department of Defense (DoD) provides guidance and enforces several mandates to ensure the government agencies plan for and manage information security. The primary purpose of the Federal Information Security Management Act of 2002 (FISMA) is to "provide a comprehensive framework for ensuring the effectiveness of information security controls over information resources that support Federal operations and assets." FISMA provides basic information security definitions, responsibilities across the government, and implications; and it designates the National Institute of Standards and Technology (NIST) to develop standards and guidelines, including minimum requirements, for providing adequate information security for all agency operations and assets, but such standards and guidelines shall not apply to national security systems. Complementing FISMA, the DoD has issued its instruction DoDI 8501.01, DoD Information Assurance Certification and Accreditation Process (DIACAP). DoDI 8501.01 provides guidance to implement FISMA and several other information assurance mandates[1] by establishing the DIACAP.

2.1 Building a Comprehensive Life-Cycle Enterprise-based Approach to Information Security

To be both operationally and cost effective, information security must be addressed at both the system and enterprise level, and must be addressed throughout the system acquisition life cycle. Such an approach can be achieved by integrating security into two independent concepts:

1. Enterprise-based risk assessment—Security risks must be assessed from an enterprise perspective continually during systems acquisition, from project conception through deployment, operations and maintenance. A representative model is defined in the Roadmap for Information Security across the Enterprise (RISE)[8].
2. Criteria-based Systems Engineering—Security requirements must be identified as part of the acceptance criteria for a system at the onset of

[1] Including DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002, DoD Directive 8100.1, "Global Information Grid (GIG) Overarching Policy," September 19, 2002, and DoD Instruction 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

an engineering effort, and tracked throughout the development process. The Vee model for general systems engineering development can be used as a representative life cycle model for illustrating the application of this concept.

Figure 1illustrates how these two concepts can be complementary to traditional C&A activities. The sections that follow describe in more detail how the concepts are applied and relate to current standards and guidance.

2.1.1 Applying Risk Assessment as part of Systems Acquisition

Information Security has a number of standard definitions which provide insight into the mechanisms necessary for a comprehensive approach. Some highlight operational aspects to information security: "The protection of information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide confidentiality, integrity, and availability."[1][2][3][4] Others highlight aspects of the requirements that must be characterized early in the acquisition effort: "Protecting information and information systems from unauthorized access, use, disclosure, disruption, modification, or destruction in order to provide—

- Integrity, which means guarding against improper information modification or destruction, and includes ensuring information nonrepudiation and authenticity;
- Confidentiality, which means preserving authorized restrictions on access and disclosure, including means for protecting personal privacy and proprietary information; and
- Availability, which means ensuring timely and reliable access to and use of information. "[1][5][6]

The objective of a comprehensive approach to information security is to measurably manage risk, that is, the process of identifying, assessing, and controlling, risks arising from operational factors and making decisions that balance risk cost with mission benefits.[7] Risk management can be measured in terms of either prevention (i.e., lowering the probability and severity of loss linked to hazards[7]), or in terms of its impact on the enterprise (i.e., "The level of impact on agency operations (including mission, functions, image, or reputation), agency assets, or individuals resulting from the operation of an information system given the potential impact of a threat and the likelihood of that threat occurring."[4]). Risk Management itself is multi-faceted and involves much more than just maintaining the information integrity, confidentiality and availability: "The process of managing risks to organizational operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system, and includes: (i) the conduct of a risk assessment; (ii) the implementation of a risk mitigation strategy; and (iii) employment of techniques and procedures for continuous monitoring of the security state of

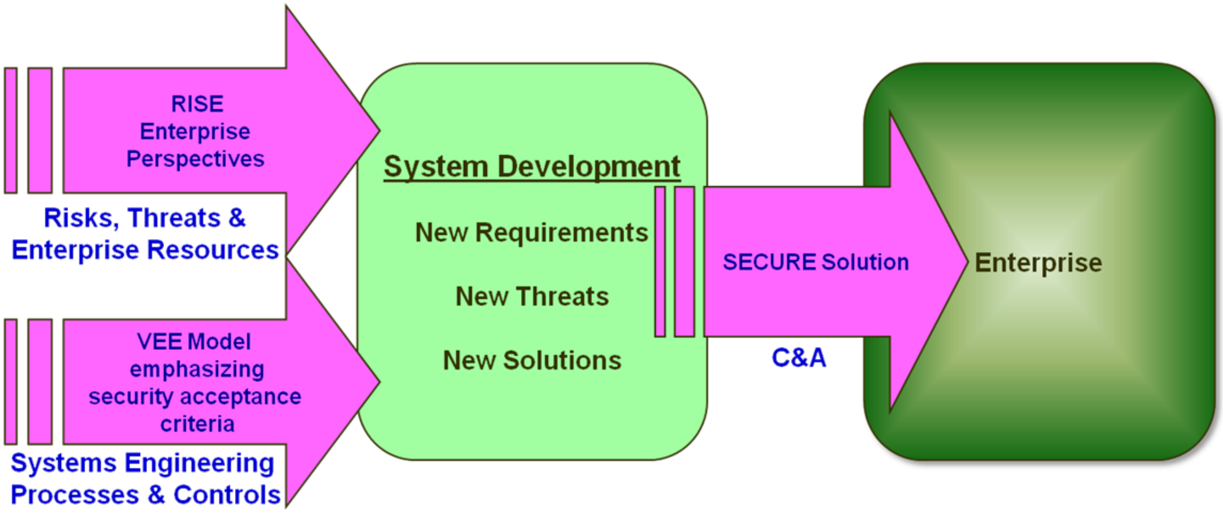

Figure 1: RISE and VEE models applied to Enterprise Development

the information system."[2]. Earlier versions of these standard definitions identified pragmatic concerns that still must be considered such as cost-benefit analysis and the consideration of effectiveness, efficiency, and constraints due to laws, directives, policies, or regulations.[1]

Few systems being acquired or developed are independent stand-alone solutions, but rather a component of an overall enterprise system of systems. Whether the capability to be acquired is a set of new or modified services, a client of existing services, a sophisticated application, or a set of databases, the context of the solution must recognize its interdependencies on the other systems that it touches, and the operational environment where the solution will be applied. A comprehensive approach to information security will recognize the security threats to an individual system and the data it manages within the context of its operational environment and the enterprise as a whole. As illustrated Figure 2, the Roadmap for Information Security across the Enterprise (RISE)[8] defines a model for managing threats, which are defined as "Any circumstance or event with the potential to adversely impact organizational operations (including mission, functions, image, or reputation), organizational assets, or individuals through an information system via unauthorized access, destruction, disclosure, modification of information, and/or denial of service. Also, the potential for a threat-source to successfully exploit a particular information system vulnerability." [4][9]

In such a model, the threats to a system are identified and assessed, and potential security controls are identified and assessed. Security controls fall into multiple classes, often reflecting operational considerations outside the technical boundaries of the IT system under development: "The management, operational, and technical controls (i.e., safeguards or countermeasures) prescribed for an information system to protect the confidentiality, integrity, and availability of the system and its information."[1][2][3][4] In some cases, existing systems or procedures in the operational environment may be sufficient to address some of the threats (e.g., firewalls, intrusion prevention systems, user authorization and authentication systems, etc.). It is essential to identify and document the threats and associated controls (assumed or planned) as requirements in the earliest stages of system acquisition.

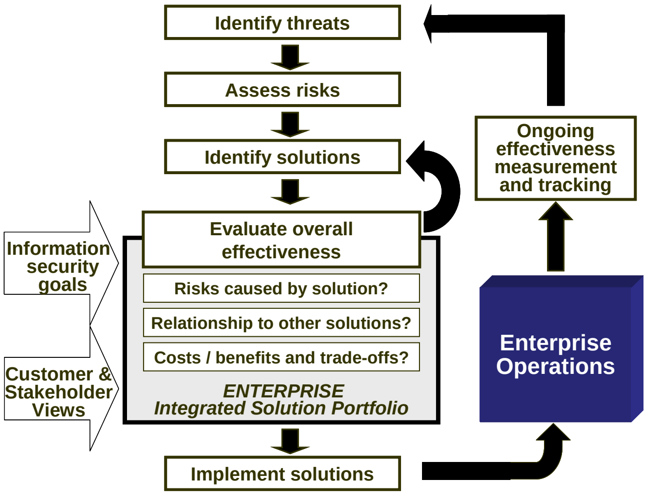
Identify threats
Assess risks
Identify solutions
Evaluate overall effectiveness
Risks caused by solution?
Relationship to other solutions?
Costs / benefits and trade-offs?
ENTERPRISE
Integrated Solution Portfolio
Implement solutions
Information security goals
Customer & Stakeholder Views
Ongoing effectiveness measurement and tracking
Enterprise Operations

Figure 2: RISE Enterprise Information Security Threat and Response Cycle

It is important to note that the RISE Threat and Response Cycle recognizes that the introduction of a new security solution (or any particular new capability, for that matter) can have an adverse impact on the enterprise security posture as a whole. Therefore, such a comprehensive approach recommends that security threats be managed at the enterprise level. The RISE methodology leverages the concept of an enterprise architecture (EA) by extending its traditionally accepted components of operational and systems views to include critical security- and privacy-oriented documentation about the enterprise. The EA acts as a knowledge base supporting technical and executive decision makers, integrating information about the enterprise mission, the organization, and its assets, as well as the decisions and plans related to them. RISE treats information security and privacy assurance as an essential enabler to effective and efficient organizational performance and mission fulfillment, rather than a constraint. Therefore, information related to security threats to enterprise information assets and the corresponding mechanisms used for assurance must be maintained and managed in accordance with their prominence.

2.1.2 Managing Security Requirements During System Development

While a focus on security requirements starting at the earliest stages of the development life cycle has yet to be institutionalized in many organizations, it is consistent with general systems development practice, as illustrated in terms of the "Vee Model"[10] in Figures 3 and 4. Security requirements defined during the early stages of analysis should be managed as any other software requirement—maintained under configuration management, associated with and/or allocated to particular elements of the solution, and eventually verified during unit, integration and acceptance testing.

During C&A, the security specialists will confirm and assess the adequacy of these solutions, whether they are inherent to the system or part of the operational environment. Finally, the "customer" (in the case of a secure system, the Designated Approval Authority or their equivalent), confirms that the software is functionally appropriate and provides adequate security to support operations.

Applying the RISE methodology and VEE Model results in the following general steps to assessing and addressing risks:

Step 1: Identify Assets. What capabilities must be protected? What data needs to be protected?

Step 2: Determine potential impact of loss of confidentiality, integrity or availability.

Step 3: Identify threats (including human, natural, intentional or unintentional, internal or external, etc.)

Step 4: Identify controls. What Management, Operational or Technical controls have to be implemented (vs. leveraging existing controls)?

Step 5: Identify and assess residual vulnerabilities.

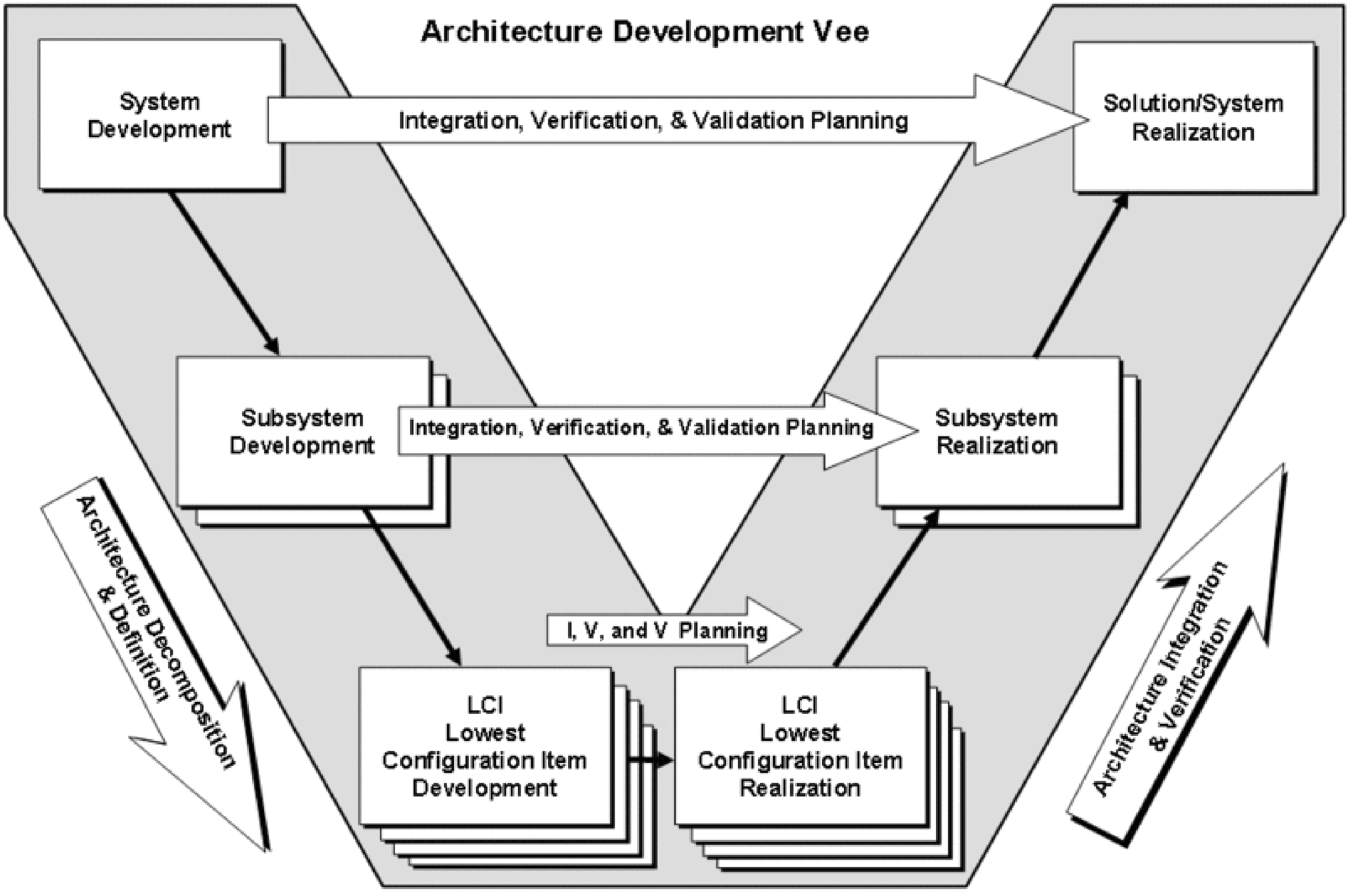
Architecture Development Vee
System Development
Integration, Verification, & Validation Planning
Solution/System Realization
Subsystem Development
Integration, Verification, & Validation Planning
Subsystem Realization
I, V, and V Planning
LCI Lowest Configuration Item Development
LCI Lowest Configuration Item Realization
Architecture Decomposition & Definition
Architecture Integration & Verification

Figure 3: Architectural View of the System Life Cycle: Analysis drives Validation Planning in Earliest Stages

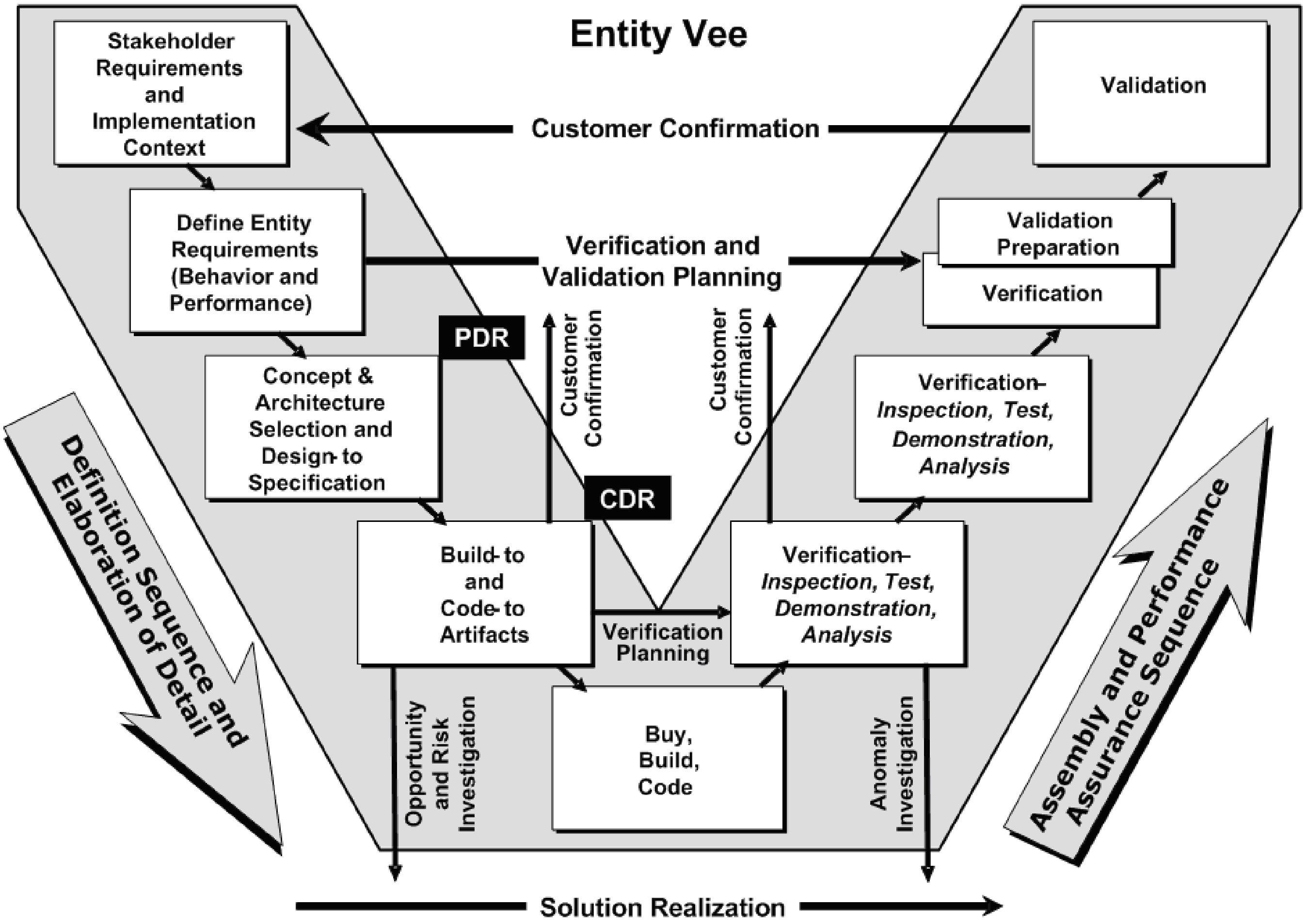
Entity Vee
Stakeholder Requirements and Implementation Context
Customer Confirmation
Validation
Define Entity Requirements (Behavior and Performance)
Verification and Validation Planning
Validation Preparation
Verification
PDR
Customer Confirmation
Customer Confirmation
Concept & Architecture Selection and Design-to Specification
Verification– *Inspection, Test, Demonstration, Analysis*
Definition Sequence and Elaboration of Detail
CDR
Build-to and Code-to Artifacts
Verification Planning
Verification– *Inspection, Test, Demonstration, Analysis*
Assembly and Performance Assurance Sequence
Opportunity and Risk Investigation
Buy, Build, Code
Anomaly Investigation
Solution Realization

Figure 4: Validation and Customer Confirmation of Requirements—Including Security

Step 6: Determine / Justify recommended additional countermeasures or accepted risks. (Accept risk; Transfer risk--e.g., to enterprise services or systems; Mitigate risk; Avoid risk--e.g., do not implement the capability).

Few systems exist or operate in isolation. While this can complicate the system development process, it can also be leveraged to support information security. Existing systems that must be integrated with the new system often have associated system documentation that can be leveraged. Properly documented system interfaces should have clearly defined security requirements for accessing those systems and their associated data. The documented security requirements for that data should be reviewed and adapted for use for the new system, ensuring that the security requirements are maintained.

The engineering process must address and account for each of the security requirements. During development, a variety of security measures (or "controls") may be applied that will contribute to the confidentiality, integrity or availability of the data and associated operations. The security controls (i.e., safeguards or countermeasures) for an information system fall into three basic categories:

- Management—security controls that focus on the management of risk and the management of information system security.
- Operational—security controls that primarily are implemented and executed by people (as opposed to systems).
- Technical—security controls that are primarily implemented and executed by the information system through mechanisms contained in the

hardware, software, or firmware components of the system.

As with any system requirement, a proper systems engineering process should explicitly document the design element that addresses the requirement, as well as the test mechanism planned for confirming that the requirement has been fulfilled. In the cases where dependencies on other enterprise systems exist, those assumptions are documented and will be confirmed during certification and accreditation.

2.2 Effective Security Certification and Accreditation

Certification is the process of evaluating a system before deployment, which is a security control unto itself: "A comprehensive assessment of the management, operational, and technical security controls in an information system, made in support of security accreditation, to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system."[1][2][4] Certification provides a comprehensive validation of the actual information assurance capabilities and services of an IT system (which in a DoD system effort would be made as part of and in support of the DIACAP), to establish compliance with assigned IA Controls based on standardized procedures. Accreditation is the subsequent process of making an authoritative management decision in response to the certification results: "The official management decision given by a senior agency official to authorize operation of an information system and to explicitly accept the risk to agency operations (including mission, functions, image, or reputation), agency assets, or individuals, based on the implementation of an agreed-upon set of security controls. "[1][2][4]

In a comprehensive life-cycle approach to acquisition and development, the security concerns and requirements for security and the anticipated controls to be applied to manage them will already be documented by the time the system enters the C&A process. The anticipated threats to operation of and the data managed by the system will be well-known (including all anticipated threats to the integrity, confidentiality, and availability, whether they be internal or external). The external systems upon which the system undergoing C&A is dependent will be identified, and associated assumptions made regarding how they impact its security profile and threats. Finally, the plans for the system to manage the remaining information security requirements will be enumerated, including all management, operational, and technical controls. These controls must be in place before C&A can be completed.

Each organization may have unique components to its C&A process, but to maintain uniformity with industry standards, most document their processes in the form of a C&A handbook based on guidance from NIST and DIACAP. The outcome of the C&A process results in a collection of documents that describes the security posture of the system(s), an evaluation of the risks, and recommendations for correcting deficiencies.

In preparing a certification package, the documents that are typically required (according to the NIST methodology) include the following:

- System Categorization Statement
- System Description with System Boundaries Noted
- Network Diagram and Data Flows
- Software and Hardware Inventory
- Business Risk Assessment
- System Risk Assessment
- Contingency Plan
- Self-Assessment
- System Security Plan

Depending on the organization and its operational requirements, other documents or variations may be required. NIST provides an excellent compendium of information security "Special Publications" that provide guidance for C&A review (as well as other information security topics).[2]

Once a Certification Package has been prepared, Mission Assurance auditors review the package

[2] http://csrc.nist.gov/publications/PubsSPs.html

and then make recommendations on whether or not the systems should be accredited according to the proposed recommendation. For the U.S. DoD, the ultimate decision is an official designation from a Designating Approving Authority (DAA), in writing or digitally signed and made visible to the DoD Chief Information Officer (CIO), regarding acceptance of the risk associated with operating a DoD information system and expressed as:

- Authorization to Operate (ATO) for 3 years,
- Interim Authorization to Operate (IATO) 180 days,
- Interim Authorization to Test (IATT) for a Specific Test Event, or
- Denial of Authorization to Operate (DATO)

All U.S. federal agencies must obtain some level of an Authorization to Operate (ATO) before their systems can be legitimately and legally deployed in an operational environment. The DAA is "The individual selected by an authorizing official to act on their behalf in coordinating and carrying out the necessary activities required during the security certification and accreditation of an information system."[1][11]

The scope to which the C&A applies is referred to as the Authorization Boundary: "All components of an information system to be authorized for operation by an authorizing official and excludes separately authorized systems, to which the information system is connected."[2][3] While this remains true when using the RISE methodology, the context within the overall enterprise is maintained. When the C&A process is completed using the RISE methodology, the contents of the Certification Package is integrated with the rest of the enterprise security documentation in the Enterprise Architecture for future reference during recertification and other systems acquisition efforts.

A key consideration for the management decisions made by the DAA involves the potentially controversial concept of determining what is considered "adequate security." Adequate security can be somewhat subjective, as it is defined as, "Security commensurate with the risk and the magnitude of harm resulting from the loss, misuse, or unauthorized access to or modification of information."[1][2] This includes assuring that systems and applications used by the agency operate effectively and provide appropriate confidentiality, integrity, and availability, through the use of cost-effective management, personnel, operational, and technical controls.[12]

Note the emphasis of cost-effectiveness in the last sentence—In many cases (and especially in a commercial environment), there is significant pressure to deploy due to production delays in development and cost overruns in acquisition. Often business managers responsible for deployment decisions may accept residual risks despite documentation thereof because any solution can be considered better than none or they consider an "80% solution" for addressing security should be good enough. To be truly cost-effective, all participants in the acquisition and/or development of a solution must be aware of their responsibilities with regard to information security, and the management and technical processes throughout the life cycle must be sufficiently rigorous to ensure that security is properly considered. The final C&A and acceptance testing process and assessment of the residual risks must support an appropriate decision by the DAA.

2.3 Comprehensive Testing to Supplement C&A

As mentioned in the discussion of the Vee Model and illustrated in figure 3, testing is not phase or activity addressed in isolation; it is a process whose requirements are initially established at the onset of the acquisition or development process, and continues throughout the development process. Acceptance test criteria, including

[3] Earlier versions of this standard referred to the "accreditation boundary" with a similar definition: "All components of an information system to be accredited by an authorizing official and excludes separately accredited systems, to which the information system is connected."[1] The more up-to-date definition differentiates between the process of accreditation and the decision to authorize operation.

information security requirements characterized within the context of the enterprise as a whole, are a product of requirements analysis. One of the primary assessment considerations for a system requirement should be, "How will this requirement be verified?" Whether a functional requirement or a security concern, attainment of a requirement will generally need to be verified through one of four methods: inspection, demonstration, test or analysis. The DoD has institutionalized some of these concepts in their acquisition processes via the Joint Capabilities Integration and Development System (JCIDS) [13]. JCIDS requires the establishment of key performance parameters (KPPs), that is, attributes or characteristics of a system that are considered critical or essential to the development of an effective military capability. KPPs are validated and included in the the acquisition program baseline.

As development continues and the design of the system emerges, the testing requirements of various components will be prescribed, both for unit testing and for integration testing. Acceptance testing should be the culmination of that process—reflecting and verifying that the system meets the operational requirements that were identified in the earliest stages of acquisition. C&A only focuses on security concerns, and when applied as discussed earlier in this paper, will account for enterprise resources and controls that are outside of the system. An effective testing strategy will apply an approach to the verification process and ensure that the testing verifies both functional and security requirements in a holistic manner. In order to ensure an enterprise perspective is applied during systems testing that will mitigate the issues discussed in previous sections, a comprehensive testing process should consider:

1. Capability testing not covered by the C&A, such as the operational environmental conditions,
2. Testing to ensure user data protection (managing personal privacy has arisen as a particular concern in the last decade),
3. Testing to ensure that sufficient protection mechanisms have been incorporated so that the operational user can identify and mitigate attacks,
4. Testing to ensure that information security controls have been implemented to protect, detect, and restore the system in response to threats, and
5. Testing to ensure that system operates compatibly and interoperates with other systems in the intended environment.

The US Government is gradually moving toward a more global enterprise perspective for its information systems management and has instituted several laws toward that goal that impact testing. The Government Performance Results Act of 1993 (GPRA)[14] and the Clinger-Cohen Act of 1996 (CCA)[4][15]. GPRA requires agencies to periodically submit a strategic plan and annual performance plans that establish performance indicators of each program activity. IT investments goals must be linked directly to the performance plans. Among other things, CCA requires the establishment of an IT capital planning and investment control (CPIC) process that will select and evaluate IT investments based on enterprise-wide criteria. CCA requires that the acquisition of systems be performance and results-based, which correspondingly implies that there be measures of effectiveness (MOEs) associated with the systems that should be considered during test planning and execution.

In response to CCA and the need to integrate security and privacy management throughout the system development life cycle, the Office of Management and Budget (OMB) has supported the development of the Federal Enterprise Architecture Security and Privacy Profile (FEA SPP)[16]. The FEA SPP provides voluntary guidance for addressing security and privacy concerns from both a systems and enterprise perspective, reflecting best practices and recommendations for security, privacy and risk management in agencies' strategic planning and investment decision processes. This guidance,

[4] The original name for this law indicates its enterprise intent: The Information Technology Management Reform Act of 1996 (ITMRA).

whether it be for risk management, management of security requirements, considerations for privacy, or applicability to an organization's enterprise architecture, can be leveraged in developing a life cycle approach and improving the test and acceptance processes.

3 CONCLUSIONS AND RECOMMENDATIONS

This paper stresses that C&A and subsequent approval for operation of a software system does not ensure adequate security. The paper provides an overview of key aspects of and considerations for a comprehensive life cycle approach to integrating information security throughout the system life cycle. Such an approach is an enterprise undertaking in itself. Proper institutionalization implies that everyone in the systems engineering process understands the overall approach and its relationship to information security; while each person understands their specialized role.

The goal of a comprehensive approach is not accreditation; the goal is an effectively operating enterprise with adequate information security. With that in mind, the process takes precedence over any particular product being acquired. Some critical success factors include:

- Identifying verifiable information security requirements (often reflecting specific thresholds and criteria) as a prerequisite to system acquisition or development.
- Clearly articulating information security requirements in capability description documents (e.g., capability descriptions associated with formal acquisition controls such as the Joint Capabilities Integration Development System (JCIDS)[13])
- Specifying Key Performance Parameters (KPPs) for addressing information security requirements during development and confirmed during testing.
- Integrating fully-accountable information security policies and procedures into the systems engineering process.
- Reviewing information security requirements and strategies as a requisite exit condition for all life-cycle control gates (e.g., system requirements reviews (SRRs), preliminary design reviews (PDRs), critical design reviews (CDRs), and test-readiness reviews (TRRs)).
- Enforcing the information security policies throughout the development, operation and maintenance of the system.
- Explicitly identifying information security requirements and design documentation that are expected to be inherited from and/or integrated into the supporting enclave, and which controls will be implemented within the system.
- Consistently incorporating information security requirements into the acquisition and contracting vehicles, including but not limited to Developmental Contracts, Service Contracts, Statements of Work (SOWs), and Service Level Agreements (SLAs).

Continuous risk management is a core process of effective information security. The authors' recommended approach to managing risks evaluates threats and strategies for responding to those threats in a systematic manner that considers the solution(s) within the context of the enterprise as a whole. Trade-offs will always be necessary to be considered by Program Managers and DAAs:

- Some controls may not be cost effective. If the cost of the control is more than the potential loss, than the risk may be accepted. This decision may be made at any time in the threat/response cycle: when considering a solution or evaluating residual risk.
- Some risks may be mitigated without necessarily eliminating the threat.
- The Program Manager or the DAA must decide if the exposure is acceptable. To make such a decision, a Program Manager should coordinate with the operational business managers (including the DAA) to ensure that the business perspective is sufficiently considered.
- But should incorporate the business perspective AND business managers in the decision.

From a process view, a comprehensive enterprise-wide systematic approach to engineering requires an integration of many disciplines and responsible parties. The Defense Acquisition University (DAU) offers a model of the development processes that incorporates details of many facets of acquisition, systems engineering, information assurance and life cycle management in a single graphic view, their Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System[18]. This chart and its accompanying documentation can be a useful resource for evaluating and institutionalizing an enterprise perspective to systems engineering and security management for any organization.

4 REFERENCES

NOTE: Content Approved for Public Release by MITRE Corporation: 11-5019--Distribution Unlimited.

1. NIST, IR 7298, Glossary of Key Information Security Terms, Richard Kissel, editor (2006).
2. NIST, Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems and Organizations (2009).
3. NIST, Federal Information Processing Standard (FIPS) 199, Standards for Security Categorization of Federal Information and Information Systems (2004).
4. NIST FIPS 200, Minimum Security Requirements for Federal Information and Information Systems (2006).
5. Federal Information Security Management Act of 2002 (FISMA). United States Code (U.S.C.) Title 44, Section 3541 (2002).
6. NIST, SP 800-66 Rev 1, An Introductory Resource Guide for implementing the Health Insurance Portability and Accountability Act (HIPAA) Security Rule (2005).
7. DoD, Joint Publication 1-02, *DOD Dictionary of Military and Associated Terms*, As amended (2010).
8. Anderson, John & Rachamadugu, Vijay, "Information Security Guidance for Enterprise Transformation," edoc, pp.459-462, 10th IEEE International Enterprise Distributed Object Computing Conference (EDOC'06) (2006).
9. Committee on National Security Systems, CNSS Instruction No. 4009, National Information Assurance (IA) Glossary, revised May (2003).
10. Mooz, Harold; Forsberg, Kevin, “The Dual Vee ––– Illuminating the Management of Complexity,” Rochester, NY: Proceedings of the International Council for Systems Engineering (INCOSE) Conference.
11. NIST, SP-37, Rev 1, Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach (2010).
12. Office of Management and Budget (OMB) Circular A-130, Management of Federal Information Resources, App. III (1996).
13. DoD, "Operation of the Joint Capabilities Integration and Development System", Chairman of the Joint Chiefs of Staff Instruction (CJCSI) 3170.01F (2009).
14. Government Performance Results Act of 1993 (GPRA), U.S. Code Title 5, Sec. 306 (1993).
15. Clinger-Cohen Act of 1996 (CCA), Title 40, Chapter 25 (1996).
16. Federal Chief Information Officer (CIO) Council Architecture and Infrastructure Committee (AIC), *Federal Enterprise Architecture Security and Privacy Profile (FEA SPP)*, version 3, sponsored by NIST, OMB, Federal CIO Council AIC (2010).
17. Defense Acquisition University (DAU), *Integrated Defense Acquisition, Technology, and Logistics Life Cycle Management System*, version 5.4 (https://ilc.dau.mil/) (2010).