TACTICAL EDGE

Customers first. Solutions that last.

July 28, 2015

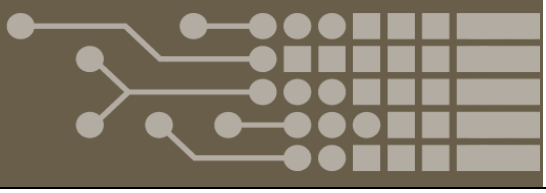
A Comprehensive Cyber Compliance Model for Tactical Systems

Meeting Army cyber security goals with an IA advocate that supports tactical system producers and consumers

Author

Mark S. Edwards, CISSP/MSEE/MCSE

Table of Contents



Problem Statement: For Army Program of Record (POR) tactical systems, achieving timely interoperability certification is impacted due to the lack of a funded, comprehensive cyber compliance program. Adding to this challenge is the need to comply with increasing and evolving cyber security requirements that must also extend beyond the test arena. To realize the Army's goal of "comply to connect, maintain compliance, and continuous monitoring," it is essential to institute a comprehensive POR Information Assurance Vulnerability Management (IAVM) program to support both functionality-focused program managers and cyber-focused operational organizations.

The Tactical Edge Solution: This paper examines a tested and verified IAVM model that Tactical Edge has successfully employed for POR systems over the past decade. This process model is designed to provide a flexible framework for management and coordination, with a goal of reducing overall program risk, improving compliance timeframes, and minimizing staff investment in support functions. A result of this process has been shown to provide a reduced certification test schedule, increase IAVA deployment and reporting options, and has enabled Tactical Edge to be an active advocate for cyber security issueses for a POR.

The three core components of the cyber compliance model define an ongoing cycle of focus areas, each supported by a clear and consistent management process.

- ✓ **Comply to Connect** is the starting point of the Tactical Edge process, with an effort to improve and document system's cyber security posture prior to connection to the network, and in an on-going basis as updates and changes occur.
- ✓ **Maintain Compliance** is the means to ensure that measures taken for security are effective, and maintain the functionality and integrity of the solution.
- ✓ **Continuous Monitoring** is integral to ensuring the integrity of the application, with a continuous feedback loop to maintain system security and accreditation.

The Tactical Edge IAVM solution brings many benefits to the POR, including a streamlined project management effort, reduced program risk, optimized accreditation management, and a clear and effective process to ensure that applications are available in the field and serving the warfighter.

Overview

Army Program of Record (POR) tactical information systems undergo Army Interoperability Certification (AIC) as a prerequisite to being fielded to Army units and soldiers. For the past 20 years, AIC events have been performed at the Central Technical Support Facility (CTSF) located at Fort Hood, Texas. Interoperability certification between the various Warfighter mission areas (i.e. command/control/communications, field artillery, air & missile defense, intelligence, sustainment, etc) involves successful validation of functional threads during the AIC events to prove capability within a system of systems. Interoperability requires, of course, connecting systems to and operating securely in an internetworked "cyber" environment.

Previous Experience

Tactical Edge has a combined 20 years experience in the following:

- Developing and fielding US Army Mission Command's Battle Command Sustainment Support System (BCS3)
- Deploying and supporting BCS3 systems to unclassified and classified networks
- Meeting evolving cyber compliance requirements for BCS3

As Department of Defense (DoD) cyber security requirements have increased and evolved, several aspects of IA management for POR systems must be considered. First, Information Assurance Vulnerability Management (IAVM) programs have remained segmented at the POR level. Second, complying with cyber requirements has impacted POR certification by levying multi-layered cyber requirements (vulnerability compliance, Host Based Security System (HBSS), and penetration hardening) as entry/exit criteria for certification, skewing program-funding priorities while lengthening development-to-test timelines. Third, cyber compliance at the time of certification does not necessarily translate down to deployed systems. Consequently, the result has been "increased vulnerability exposure, unclear roles and responsibilities throughout the IAVA process, poor communication distribution notification throughout the IAVA process, lack of standardization of tools, repositories, and contract language, policy gaps and insufficient staffing of policies, and insufficient resources required to execute the IAVM mission for tactical and enterprise systems".

To realize the Army's goal defined by the CIO/G6 as "comply to connect, maintain compliance, and continuous monitoring," instituting a consolidated IAVM program applicable to the majority, if not all, of POR systems is essential. This IAVM program should include the plans, procedures, processes, resources, and authority required to achieve the stated Army objectives. For POR tactical systems that support the Army's ability to fight and win wars, this means committing to an IAVM model that encompasses the lifecycle of these systems from development, certification, and deployment, including both intermittent and continuous operation models. To date, IAVM programs have been managed by each POR in conjunction with various stakeholders deployed. The stakeholders impose requirements on the system owners and users to connect and maintain connections to the DoD Information Network (DoDIN), and these requirements vary across each operational environment and Program Executive Office (PEO). A *comprehensive* cyber program designed not only to improve POR development and certification efforts but also acting as a focal point for all stakeholders focused on cyber security for POR systems will benefit all parties, as well as the POR itself.

Recognition

Tactical Edge has been singled out in the following:

Tactical Edge has defined the US Army Mission Command's Battle Command Sustainment Support System (BCS3) Information Assurance Vulnerability Management (IAVM) needs, and successfully collaborated with multiple parties to ensure these needs were met in a timely and effective manner.

This document examines a proven IAVM model that supports the requirement to "comply to connect," then identifies options to improve the model's ability to "maintain compliance," and lastly, addresses the impacts to development and certification related to "continuous monitoring." For a system to "comply to connect," DoD standards are employed to verify Security Technical Implementation Guides (STIG) and IAVM compliance and navigate the Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) / Risk Management Framework (RMF) process to obtain an Authority to Operate (ATO). Maintaining compliance is an ongoing process, and requires meeting mitigation timelines for applying IAVA updates while performing annual review of ATO artifacts. While continuous monitoring imposes integration and procedural validation of HBSS and ACAS deployment with respect to POR systems, it also implies that these measures improve system hardening against penetration exploits, which has become another aspect of certification. POR program managers need a standard penetration methodology in the context of other defense-in-depth measures to articulate risk level and have confidence in system hardening prior to independent penetration testing.

Comply to Connect

At the heart of 'comply to connect' is an IAVM compliance model designed, implemented, and proven effective over 10 years. This model has been responsive to changing vulnerability assessment standards and mitigation requirements identified in Army Computer Emergency Response Team (ACERT) alerts. Unlike most other POR systems operating primarily on the SIPR network, the Battle Command Sustainment Support System (BCS3) program has a complex architecture including enterprise servers and tactical laptop clients operating on NIPR and SIPR networks since 2004. Because of this exposure to NIPR network operations for in-garrison and theater deployed systems, especially when compared to other tactical systems operating primarily on SIPR tactical networks, the Tactical Edge IA lead developed an in-house BCS3 IAVM program to improve on the CTSF quarterly IAVA patch distribution schedule and meet customer needs. A team may not choose to delay IAVA mitigation, and to simply promise to mitigate open vulnerabilities with the next quarterly IAVA patch, as this will not satisfy network connection requirements. Instead, the team and model are designed for an active and proactive approach towards vulnerability and risk management. The individual tasks in the Tactical Edge compliance model, illustrated in Figure 1, are found in many parts of the solution process, and focus on both the technical and non-technical aspects of reaching a compliant state. These efforts include task management, teamwork and coordination, and the implementation of the technical tools required to ensure clarity and accuracy in the information systems management, and across the entire security management lifecycle.

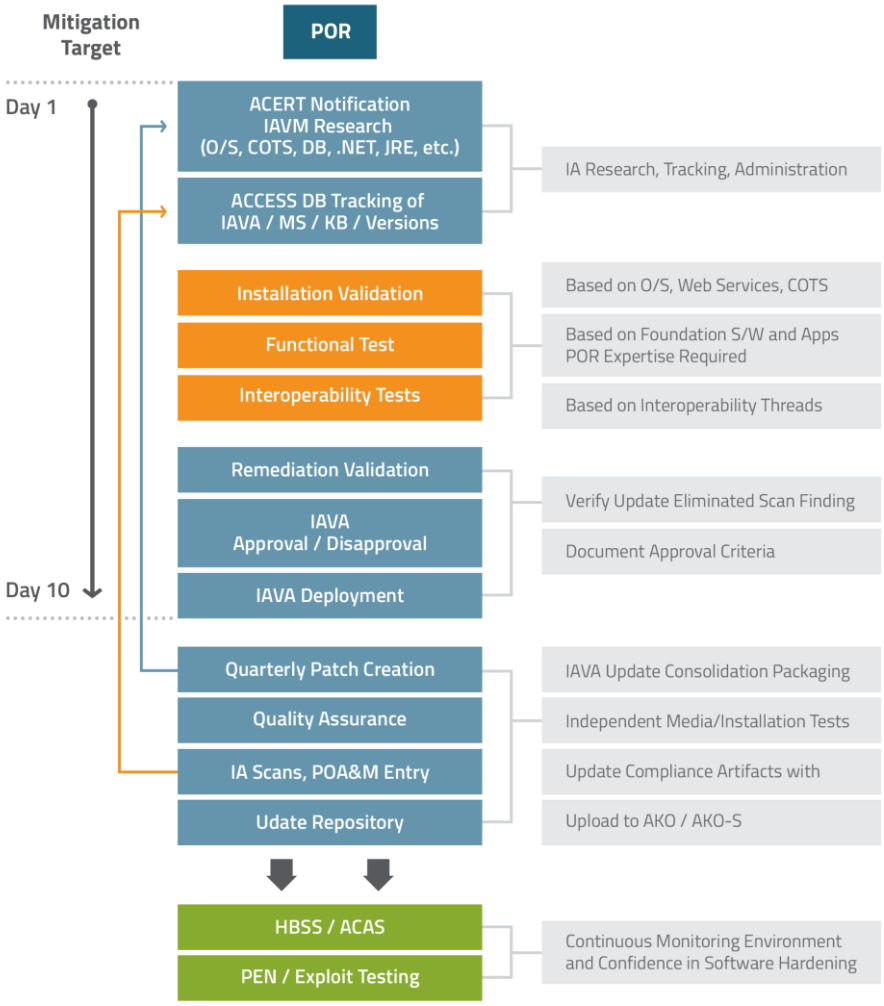


Figure 1. IAVM Compliance Model

Maintain Compliance

The Tactical Edge IA management process views the maintenance of a system's compliance, and thus it's accreditation, as a direct following from the initial "comply to connect" effort. This effort moves beyond the initial testing and documentation required to comply with domain or enclave requirements, and incorporates the security management lifecycle to maintain and enhance the overall system security. The Tactical Edge model is designed to leverage economies of scale for common tasks, such as research, issue tracking, community engagement, patch development, and reporting. Other resources leveraged in this model would include IA-credentialed personnel with POR technical expertise and access to POR systems within the interoperability test facilities that exist at the CTSF. This model is a natural home to support ATO actions (DIACAP or National Institute of Standards and Technology (NIST) Risk Management Framework), provide Plan of Action and Milestones (POA&M) inputs, and maintain other cyber related documentation for every system. Tactical Edge has used this model in support of past DIACAP actions leading to BCS3 client and server enterprise ATOs by supporting Agent for Certifying Authority (ACA) and Certifying Authority (CA) reviews, updating supporting documentation, and supporting other needs of the Information Assurance Security

Officer (IASO) project lead. As RMF evolves to replaces DIACAP, resources associated with this type of IAVM model will be invaluable to standardizing IA actions, reducing costs, and providing better service.

The compliance management function emphasizes teamwork, collaboration, and coordination across many entities to continue to be successful on a daily basis. Although technology platforms are critical, and provide essential capabilities in the distribution of software patches/updates, maintaining configuration management, and in auditing application platforms, the segmentation between technology solutions and process for execution causes gaps and delays. The compliance management model integrates the team-centric elements into a cohesive and manageable view. Taken together, the result is a rich and comprehensive approach towards compliance management that ensures the full system availability and integrity.

Continuous Monitoring

Monitoring a system is a constant effort, blending technology with staff expertise, and supported by an efficient and open process. The Tactical Edge IA management process focuses on the effective joining of each of these areas in order to provide a comprehensive solution, and to avoid gaps or issues with the system security and compliance.
The technical aspects of system monitoring are accomplished through a variety of mechanisms. Host based monitoring, implemented to be compliant with DoD continuous monitoring requirements is comprised of a series of Host-based Security System (HBSS) modules installed on POR systems and managed by an associated HBSS Enterprise Policy Orchestrator (ePO) server. Systems must be configured to allow scanning from an Assured Compliance Assessment Solution (ACAS) scanner. Other host security software may include anti-malware software, anomaly detection capabilities, and other security-centric applications.

The technical aspects of the solution, however, are only part of the overall compliance capability. The understanding of the system functions and capabilities, and how these capabilities are supported or impacted by security activities must be well understood by the broader team. Each response to an IAVA must factor in system operation and functional considerations, and be closely coordinated between all parties. In this area the Tactical Edge process excels, ensuring that all key POR representatives are fully engaged in the monitoring process, and part of the response decision-making efforts.

For BCS3, the Tactical Edge team has demonstrated this depth of experience in applying the continuous monitoring process to both enterprise and tactical systems. In many cases, the change of the operating enclave and the changes in associated security policies impacts a system's ability to execute. The combination of well-documented test scenarios and a fully capable test lab enables the team IA analysts to verify configurations and policies prior to deployment, and to avoid system failures or loss of service.

Tactical Edge Cyber Compliance Solution

The Tactical Edge cyber compliance model is a solution to meet these requirements, and to do so in a constantly changing and challenging environment. This process is a multi-step effort designed to coordinate initiatives between team members, provide maximum visibility on IA-management efforts, and to produce the highest security result for the customer and warfighter.

(1) Research, Tracking, and Management

A key aspect of the IAVM process is to maintain current information and awareness of risks and threats to all systems. This IAVM process begins with IAVA research consisting of subscribing to ACERT alert notices and routinely checking various CAC-enabled update sites and patch repositories including Defense Information Systems Agency (DISA), Army Network Enterprise Technology Command (NETCOM), Army IAVM, and NIST. ACERT notices include the IAVA's pertinent information such as issuing authority, impact, compliance/regulatory/non-compliance requirements, affected software and patches, required actions, and patch resources. The relevant point here is the applicability of an IAVA to a specific POR baseline based on software version, operating system, and applications. A feature rich tracking application or database is extremely important for managing this largely administrative task and should have user definable reporting and data export capabilities. The ***benefit*** to the program and the team is ***greatly improved knowledge dissemination***, and the ability to ***manage risk in a real-time basis***, as opposed to responding to threats in an unplanned and ad-hoc manner.

(2) Functional and Interoperability Testing

The ability to consistently and completely test a system is a critical step in the management of the system integrity and security. This capability is important not only to validate general system functioning, but also to be able to meet short mitigation timelines with minimal system impact. An IA focused test team must have the POR subject matter expertise and technical skills to recommend IAVA approval based on defined test criteria. A deterministic set of test procedures developed and approved by the POR software developers and subject matter experts (SMEs) are designed to efficiently test software capabilities within a specific timeframe based on the IAVA updates relationship to core software dependencies. The Tactical Edge process recommends grouping and organizing application and security tests to allow for both high-level and targeted tests. When performing an update of an infrastructure component, this range of test cases allow for the impact of the update to be rapidly assessed, and for the IAVA response to be completed as quickly as possible. An extended set of test cases are also defined to consistently step through core application procedures that test specific feature, again within a targeted timeframe. The IAVA process efficiency and corresponding test cases help to manage expectations, allocate resources required, and to ensure a successful outcome in the IAVA response. The end result, and net benefit, to this testing process is a system will be properly and consistently maintained, with updates and IAVA remediation deployed in a quick and responsive manner, all while validating end-to-end functionality provided by the application.

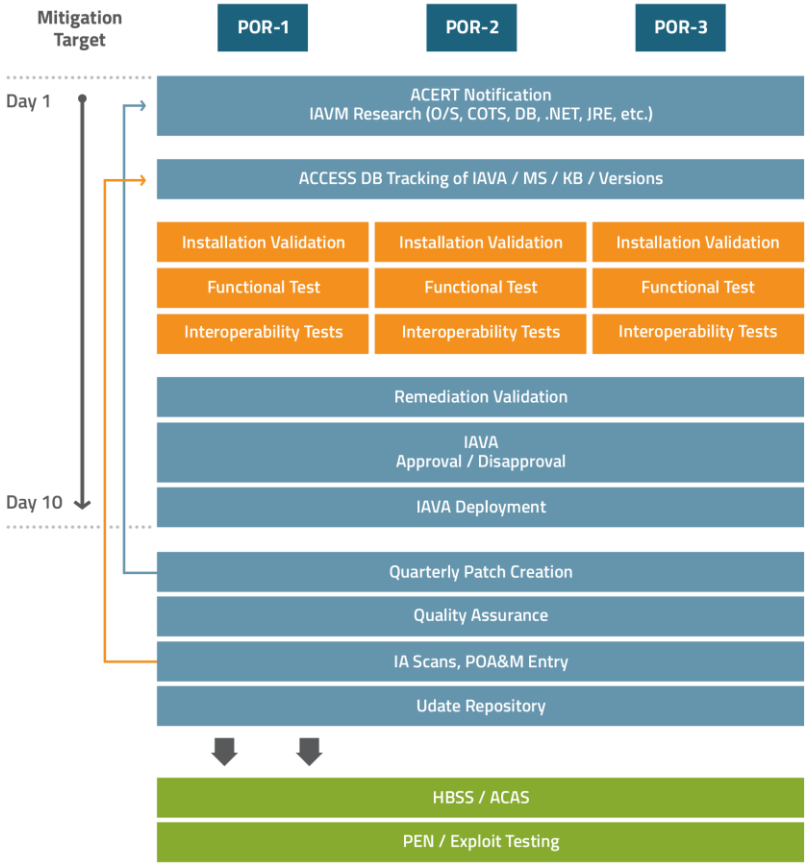


Figure 2. Expanded IAVM Model

(3) IAVA Approval and Deployment

A critical function in the IA process, and to support the program in an effective and timely manner, is the close teamwork and coordination of the IA and POR SME for IAVA assessment, remediation, and approval. This close coordination builds on the depth of experience available from team members, and ensures that this time-critical process is executed as quickly as possible. The team works in lock step to test and verify solution compliance by executing multiple steps: ranging from a vulnerability scan using automated tools, such as STIG Compliance Checker (SCC) or Assured Compliance Assessment Solution (ACAS), to the software modifications and system updates to remediate the findings.. This coordination enables the team to provide a direct path forward for each IAVA, in order to clearly communicate this solution to POR system users and other interested parties. The resultant benefit of this team-focused approach is the minimized timeline for IAVA response, the increase in overall compliance, and the improvement in communications to team members and the POR community.

(4) Patch Creation and Deployment

The Tactical Edge IA management process is executed in an agile manner; able to meet rapid turnaround response requirements, while the process also focuses on ensuring the maintenance and sustainability of the system on a long-term basis. To accomplish this, the team recommends the creation of quarterly patch updates, packaged to simplify and streamline the distribution and installation of these essential elements. Each quarter, the team bundles approved

IAVA updates into a single, comprehensive installation package. This package is used to update and verify system functioning and integrity prior to distribution to the POR community, and provides a clean baseline for systems maintenance at all operational levels. An example of this effort was the BCS3 Software Update Tool (SUP), which incorporated key IAVA patches and updates into a self-contained and easily distributed installation bundle. Users and administrators may use this bundle to ensure that all patches and updates have been installed, reducing the risk of missed vulnerabilities and reducing the manpower required to maintain the system. The team recommends moving beyond manually installed updates, with an automatic update solution that will distribute and verify these patch bundles to all operational instances in a timely manner. The net result of this process is the benefits of improved compliance, a verifiable security baseline for operational systems, and a reduction in ad-hoc patch management and distribution for application administrators.

(5) Security Management Lifecycle

The ability to respond quickly to events, and to distribute updates to systems are critical and essential components of maintaining the IA posture of a system, however these must be performed in context to the management of the overall security management lifecycle. The Tactical Edge IA process considers the ongoing compliance management factors, such as system verification, ongoing validation, and technology insertion as key elements in maintaining system security. In order to create a platform to support this effort, Tactical Edge has created a cyber lab, in support of projects such as BCS3, designed to test, integrate, and deploy new tools and techniques to continually improve the overall security of a solution. The cyber lab conducts tests using software and patch distribution technologies, such as Windows Server Update Services (WSUS), System Center Configuration Manager (SCCM), and other automated solutions, to better determine the state of individual deployments. Vulnerability scanners, software penetration tools, and policy management solutions are used to continually test and verify compliance to past IAVAs, and to be prepared to meet emerging threats. A strategy of defense in depth, and continual testing, ensures that solutions are optimized to meet both the security and functional requirements of the customer.

As shown in Figure 2, the Tactical Edge security management lifecycle process is modular, enabling the expansion and flexibility to incorporate new technologies, threats, and risk management requirements in an ongoing basis. This process builds on a generic process core, upon which system-centric additions and extensions are added. These customizations are incorporated into the overall framework of execution, while drawing on a process created through the depth and experience of the team members. This model is continually reviewed and enhanced, ensuring that customers receive current and relevant solutions, have a clear and consistent process for execution, and minimize system and program risks for noncompliance.

Conclusion

Improving IAVA compliance for POR tactical systems necessitates adopting a complete and holistic IAVM model for as many systems as possible, while incorporating all aspects of system security lifecycle management. While each program has some form of security management, Army review has shown them lacking as a whole. The Tactical Edge cyber compliance solution is a model with a proven track record, and is implemented by a cyber-certified, POR-expertise team. This model brings benefits beyond standardizing IAVA compliance, including macro-level risk management, deeper program management insight into operations, and the ability to scale compliance and assurance operations to all deployment areas. Using the Tactical Edge compliance model, the POR IAVM entity will become the IA focal point to help reduce IA impacts on certification test schedules, define and support IAVA deployment and reporting options, and support external agencies for cyber matters relating to POR systems.