

Information Assurance Management Process Automation Abstract

Information Assurance Management is a critical yet complex and labor-intensive business function. There are many individual business processes that make up an overall Information Assurance Management Program such as.

- C&A: to address Federal Mandates (C&A, Risk Assessment, FISMA Reporting)
- Continuous Assessment: to address requirements for on-going C&A maintenance (i.e., Continuous Monitoring defined in NIST 800-37 and post-accreditation, defined as Phase 4 in DITSCAP and NIACAP). Continuously manage risk and compliance posture and/or maintain currency of your C&A program
- Inventory and configuration management
- Security compliance testing
- Risk assessment
- Vulnerability management
- Incident management
- Vulnerability remediation
- Patch management and distribution

Security professionals using manual methods typically execute these business processes. A manual approach to such a complex and important business function (i.e., Information Assurance Management) does not provide for efficiency, consistency, repeatability, or accountability. Furthermore, due to the high cost of security professionals, this model does not scale well. Manual Information Assurance Management processes result in inefficiencies and high labor costs. Meanwhile, as the need for more support increases, organizations are under increasing pressure to do more with less.

Due to the importance of information security in today's business environment, there is a need to treat Information Assurance as any other critical business process. There must be consistency, repeatability, and accountability. Also, it's no longer good enough to know that you have a particular security problem. Remediation must also be part of the end-to-end process. Problems must be fixed quickly, the fixes must be validated, risk and compliance posture must be recalculated, and managers must be notified of status.

Because budgets are under constant scrutiny, it is not reasonable to expect that labor funding will continue to increase from year to year. Automation is the key as it serves to reduce labor cost and provides for the consistency, repeatability, and accountability that is so important in critical business processes like Information Assurance Management.

Organizations today employ many different people performing a wide range of tasks and who use many different standalone systems to achieve their Information Assurance Management objectives. There is a need for Information Assurance Management process automation that will allow all of the various people and business systems that make up a Information Assurance Management program to interact with each other as one seamless, efficient, and repeatable business process. Such automation will serve to improve organizational efficiencies and reduce lifecycle costs associated with Information Assurance Management by decreasing an organizations reliance on expensive security professionals. Additionally, such an automated approach will greatly improve organizational security posture because automation will allow security issues to be understood and addressed more quickly than is possible using purely manual methods and un-integrated business processes.