



FISMA: More than Just POA&M Reporting

Xacta IA Manager™ Helps Agencies Ensure Continuous IT Security as Required by FISMA's NIST Regulations

An Xacta White Paper

December 2004

Introduction

The passage of FISMA has resulted in an extensive set of NIST regulations for IT risk compliance and assurance. Some agencies are taking a very narrow view of FISMA by focusing on its periodic reporting requirements through the completion of basic Plans of Action and Milestones (POA&M), perhaps because OMB has threatened to withhold funding for projects when agencies fail to report properly.

But FISMA is really much more about *security management* than it is about POA&M reporting. The bigger FISMA picture includes NIST's development of standard controls, processes, and guidance for certification and accreditation (C&A), or risk management and security management in general. In their consideration of FISMA reporting tools, agencies should be sure to look beyond "mere reporting" to address other aspects of FISMA compliance.

Many recently developed FISMA reporting tools are informal government/contractor collaborations that require continuous care and feeding to ensure future lifecycle support is maintained. On the other hand, commercial off-the-shelf (COTS) products are more formalized in their development and support methods. When considering any software-based solution, agencies should be sure to examine the long-term viability and professional support structures of all potential solutions. Several offerings in the market have informal, ad-hoc product development and support methods that lack a long-term plan and require very expensive, on-site consultant engagements to support their application. In the long run, it is more effective to procure a COTS offering that has a proven support track record.

Xacta IA Manager: A Proven COTS Solution for Information Assurance

An example of such a COTS solution is Telos Corporation's Xacta IA Manager, which has been in use by federal agencies for information assurance since 2000. Xacta IA Manager enables federal agencies to comply with FISMA/NIST security and C&A reporting requirements, and automates many functions associated with information assurance such as:

- Asset information gathering

-
- Risk calculation
 - Generation of a Security Requirements Traceability Matrix (SRTM) and Security Test & Evaluation (ST&E)
 - Automated security testing
 - Document publishing
 - POA&M reporting (data pulled from system C&A data files)

Agencies using Xacta IA Manager report that this automation can reduce overall C&A efforts by up to 70 percent. Additionally, Xacta IA Manager's Process Enforcement Edition enables an agency to institutionalize and automate certain remediation plans and processes via workflow technology, allowing the agency to address OMB requirements for security remediation plans and demonstrating progress toward these plans.

Key Requirements for Meeting an Agency's Unique IT Security Management Requirements

As a solution for automating risk compliance and assurance management, Xacta IA Manager enables agencies to generate documentation for both C&A and FISMA reporting according to each agency's unique requirements. A key element for this is the ability to provide role-based system-of-systems visibility across the enterprise. Xacta IA Manager can aggregate system risk and compliance information to provide overall status for the enterprise. It is also possible to drill down into the sub-organizations, the systems that make up the sub-organizations, the devices that comprise the systems, the specific failed requirements and vulnerabilities associated with each device, and plans for remediation.

A second key area of flexibility is the ability to generate standard reports, and especially to accommodate proprietary reporting systems or formats already used by an agency. Xacta IA Manager includes more than 100 regulations and policies for IT risk compliance and management, and it is regularly updated so that its pool of standards is never obsolete. These include agency-specific regimens such as Treasury 8510, DOJ 2640.2, as well as government-wide initiatives such as GAO FISCAM, the NIST 800 series, FIPS 199, and the pending FIPS 200.

When an agency has its own unique evaluation criteria and reporting requirements, Xacta IA Manager can be configured to accommodate those as well. For example, the IRS has configured Xacta IA Manager to utilize their unique baseline security requirements (BLSRs) as their information security requirements, added the requisite test plans and procedures, and developed customized risk assessment reports to identify and report on existing and potential threats, vulnerabilities and the effectiveness of the current and proposed safeguards.

Xacta IA Manager enables C&A and FISMA to be synchronized, satisfying the reporting requirements for both C&A and FISMA and improving the quality and consistency of output. This is especially valuable when an organization has a C&A team and a separate

group responsible for FISMA reporting. Furthermore, Xacta IA Manager can eliminate the need for other FISMA-specific reporting tools, saving additional costs.

Xacta provides a robust Plan of Action and Milestone processing framework. POA&M elements can be automatically imported from the C&A results and evaluated on a case-by-case basis, as shown in Figure 1. This data is captured for each system within Xacta IA Manager and reports can be generated for each system or for the entire agency.

The screenshot shows a web browser window titled "Edit Plan of Action Item 'Encryption' - Microsoft Internet Explorer". The form contains the following fields:

- Title***: Encryption
- Creation Date**: 10/26/2004
- Weakness**: [Test: 20162 - Controlled Communication] Encryption algorithm is not NSA approved.
- Point of Contact**: Jim Smith
- Resources Required**: 40 Hours engineering support, 80 Hours project management support, 60 hours system administrator support
- Scheduled Completion Date**: 31 January 2005
- Milestones with Completion Dates**: Complete Design Plan 15 November 2004, Install software upgrade 15 December 2005, Test application and related system 15 January 2005, Deploy into production 20 January 2005
- Changes to Milestones**: none
- Audit/Review Status**: reported to IG
- Overall Status***: Ongoing

Figure 1: POA&M Element Detail

Xacta IA Manager is the only commercially available product that is able to turn the traditional static C&A process into an automated continuous risk management process to satisfy NIST 800-37. For this reason, Xacta IA Manager greatly improves the overall value of C&A by providing organizations with a dynamic view of risk and compliance over time. Additionally, Xacta IA Manager significantly reduces the cost of re-accreditation and FISMA reporting as much of the data collection, risk and compliance re-calculation, and reporting work is performed automatically over time.

The screen capture in Figure 2 shows an internal executive, roll-up report of FISMA compliance. As indicated by the button at the top of the screen, Xacta IA Manager

allows this data to be exported into MS Excel spreadsheet format in the layout expected by OMB:

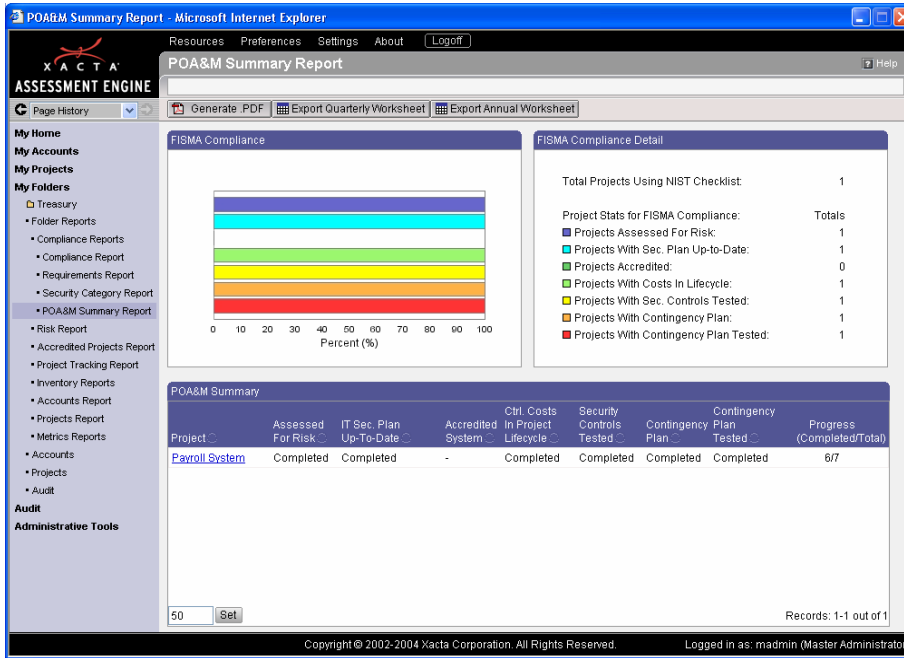


Figure 2: Enterprise FISMA Reporting

Figure 3 shows the same data exported to an MS Excel spreadsheet:

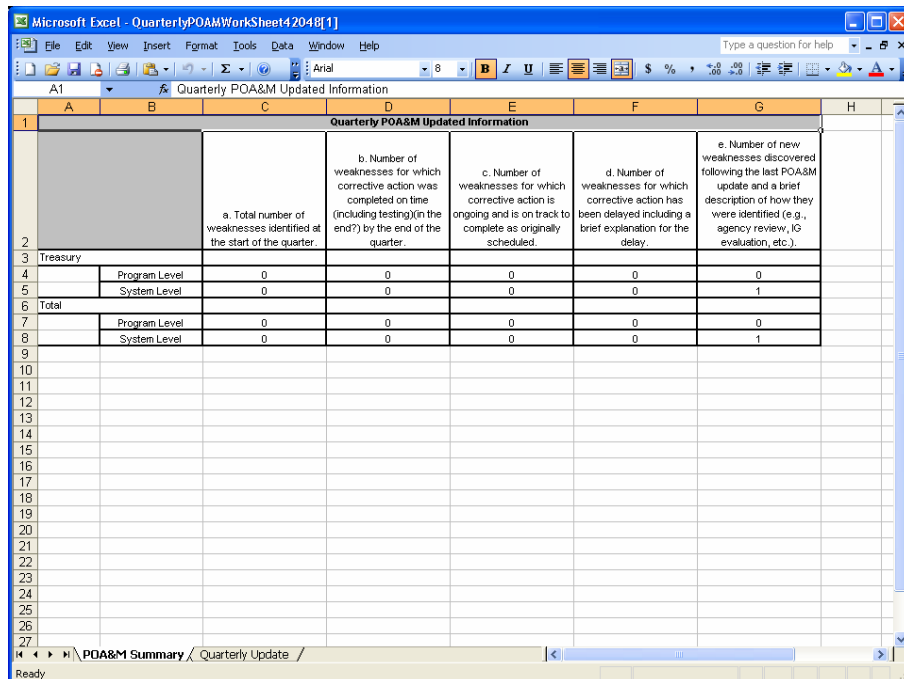


Figure 3: Exporting FISMA Data to MS Excel

Powered by Intellectual Capital

To maintain the Xacta IA Manager knowledge-base of NIST and agency-specific security policies and regulations, Xacta employs a full-time staff of dedicated information security analysts. This core, internal cadre is surge-augmented by members of the Xacta Information Assurance professional services team who are customer-facing consultants and typically the first to obtain the latest customer-modified regulations. Xacta follows a structured process of parsing regulations into security domains and security categories. The next step is either to associate existing test procedures or to write new test procedures for each of the parsed requirements. The test procedures for a particular requirement are actually a group of procedures that are categorized based on scope of influence, equipment classification, and software application/operating system applicability. The content is delivered to the customer population within baseline templates that are electronically updated through the Xacta ActiveUpdate service.

Requirements for a Complete Solution

As discussed earlier, a comprehensive solution should look beyond mere FISMA reporting to consider a broader FISMA solution. Any C&A/FISMA solution should provide these minimum capabilities:

- Certification & Accreditation automation to include both NIST 800-37 and DCID 6/3
- Robust and extensible content knowledgebase that includes federal and industrial policies and regulations, such as GAO FISCAM, OMB A-130, DOJ 2640.2, Treasury TDP 8510, NIST 800-53 and 53a, etc.
- Open framework for content knowledgebase customization including multiple levels of testing
- Complete C&A reporting for NIST, NIACAP, and other formats
- Automated generation of C&A Test Plans with detailed test procedures
- Import/Export of the formal test plan and associated procedures
- Automated execution of test plans and procedures using Xacta Detect
- Integration with vulnerability scanners — NESSUS and ISS Scanner
- Integration with asset inventory repositories — MS-SMS and Tivoli
- Integral risk algorithm to automatically calculate risk levels based on threats, vulnerabilities, and asset importance
- Risk analysis framework to ensure the security analysts provide necessary evidence/justification for the statement of residual risks
- Integration of the C&A risk elements with POA&M elements
- Import/Export of POA&M elements from C&A process
- Continuous Monitoring functionality to support the post-accreditation phase of the C&A lifecycle (or operational phase of the system lifecycle)
- Integral asset discovery feature with rogue server detection and notification.

The following security features and assurance requirements should be added for the potential evaluation of any FISMA solution:

- Proven identification and authentication (I&A) mechanisms
- Proven discretionary access control (DAC) with the application
- Role-based access control to project data based on role-defined privileges
- Separation of the audit log access/control from administration accounts
- NIAP certification of the vendor's solution
- Demonstration of documented software configuration management practices
- Evaluation and exercise of the vendor's technical support infrastructure

Xacta IA Manager meets these and many other agency requirements.

Summary

Xacta IA Manager has been proven in more than 300 implementations as a powerful yet flexible and user-friendly application. It offers wizard-driven C&A process automation and automatic report publishing features that greatly reduce the time and effort required to comply with C&A and FISMA reporting requirements. Upon completing baseline assessments, it can be configured to continually and automatically update risk and compliance posture as well as corresponding C&A and FISMA documentation.

Its latest release includes enhancements for ease of installation, configuration, and use, including:

- Enhanced installation utility that provides users with three installation options, including: 1) streamlined installation for single-server or workstation environments; 2) easy-to-use, automated upgrade process for existing customers; and 3) custom installation for users wanting to install the application across multiple servers
- Quicker access to executive-level security status information presented in an easy-to-read graphical format that includes assessment expirations and objectives, as well as current system status details
- Greater flexibility in engaging Xacta's patent-pending Continuous Assessment feature to automatically and simultaneously collect asset information across multiple network segments

As evidence of Xacta IA Manager's ease of installation, configuration, and management, the Census Bureau recently acquired it to help automate security management for both C&A and FISMA reporting. Using a centralized server approach, Xacta IA Manager was installed and configured in less than a day, enabling bureau personnel to do basic projects that same day.

Xacta IA Manager is available in five levels of functionality, so minimum installation and configuration is determined by how comprehensive you need your IT security capabilities to be.

Xacta IA Manager has also been evaluated and proven compliant with a number of customer-driven requirements, including Section 508 compliance, NIAP compliance, and compliance with agency enterprise architectures. Employees with visual impairments at the U.S. Department of Education extensively tested Xacta IA Manager to ensure its accessibility. Xacta IA Manager has completed and passed the formal testing milestone within the NIAP certification process; the final certification report should be issued by the end of 2004. The Xacta software has been deployed and undergone a variety of certification and accreditation processes in the Department of Defense, Department of Homeland Security, Internal Revenue Service, within the intelligence community, and many other federal agencies.

About Xacta

Xacta Corporation, a Telos company, develops, markets, and sells government-validated secure enterprise solutions to federal, state and local agencies, as well as to commercial customers. Xacta's offerings include enterprise IT security management solutions, enterprise security consulting services, enterprise messaging, secure wireless networking, and high assurance credentialing solutions. Its solutions are represented to the federal government on Telos' GSA schedule.

For more information about Xacta IA Manager and other secure enterprise solutions from Xacta, please contact us:

Toll-free: 1-877-40XACTA

E-mail: info@xacta.com

Web: www.xacta.com

© 2004 Xacta Corporation. All rights reserved. Xacta IA Manager is a trademark, and Xacta is a registered trademark, of Xacta Corporation. All other trademarks or registered trademarks belong to their respective owners. Xacta is a subsidiary of Telos Corporation.