The NIST Risk Management Framework for DoD IT

Smooth your transition from DIACAP to the NIST RMF with Telos process experts and the Xacta® suite for risk-management automation.

Telos® Corporation is a federal market leader in assisting customers in the Intelligence Community and the Department of Defense with the transition to the NIST Risk Management Framework (RMF). As a solution partner, Telos has helped multiple and diverse agencies move from previous regulations (DIACAP, DCID 6/3, JAFAN 6/3) through a paradigm shift into the new "risk aware" methodology. Our experience will prove invaluable in your transition to the NIST RMF for DoD IT.

Telos has been providing training and transition support to the IC and DoD since the signing of ICD 503 in September 2008. As a result, we have considerable experience customizing implementation plans for organizations moving to the new framework. We've developed the training and transition support processes to help your information assurance workforce adjust their practices to align with the NIST RMF. And we've built valuable enhancements and new functionality into Xacta, our solution for security risk management automation.

Xacta 360: More than Just a Repository.

Xacta 360, the core component of Xacta, is more than just a passive repository for security feeds. It enables critical functionality to maintain an updated Body of Evidence (BOE) within the NIST RMF assessment & authorization (A&A) process. A few of these time-saving capabilities are:

- **Automated Categorization** – Xacta 360 maintains up-to-date regulatory content including the NIST 800-60 Library of Information Data Types. This enables Xacta users to quickly and efficiently categorize systems working from an agency or organizationally pre-determined baseline. Agencies or organizations can also modify or create new data types for inclusion in their categorization processes.

- **Multiple Inheritance** – Many providers can satisfy either single or multiple controls, but Xacta 360 is the only product that supports multiple inheritance. Xacta 360 maintains a persistent awareness of the relationship between systems that have been selected to inherit or provide controls and notifies all necessary parties when a control needs to be updated or has failed an assessment.

- **Overlays and Supplemental Guidance** – Xacta 360 is the only solution that enables the user to build or select from pre-determined situational controls (overlays). When the selection of an overlay conflicts with a system's categorized baseline, Xacta 360 allows the user to select which is best for the situation while documenting the decision and rationale. In addition, when an overlay provides supplemental guidance, Xacta 360 appends it to the baseline implementation guidance, enabling the system developers to quickly and easily understand how to best meet the regulatory control.

Xacta 360 not only fully automates the NIST assessment and authorization process while dynamically building your body-of-evidence documentation, it has also been enhanced with the critical functions you need to maintain your authorization:

- *Automated Categorization*
- *Multiple Inheritance*
- *Overlays & Supplemental Guidance*
- *Push-Button Regulation Transition*

- **Push-Button Regulation Transition** – With the push of a button, Xacta 360 can update a current A&A effort's regulatory content. After an organizational mapping has been completed, the system translates old DIACAP packages to new NIST packages – correlating the corresponding controls, test plans, and results between the standards accordingly.

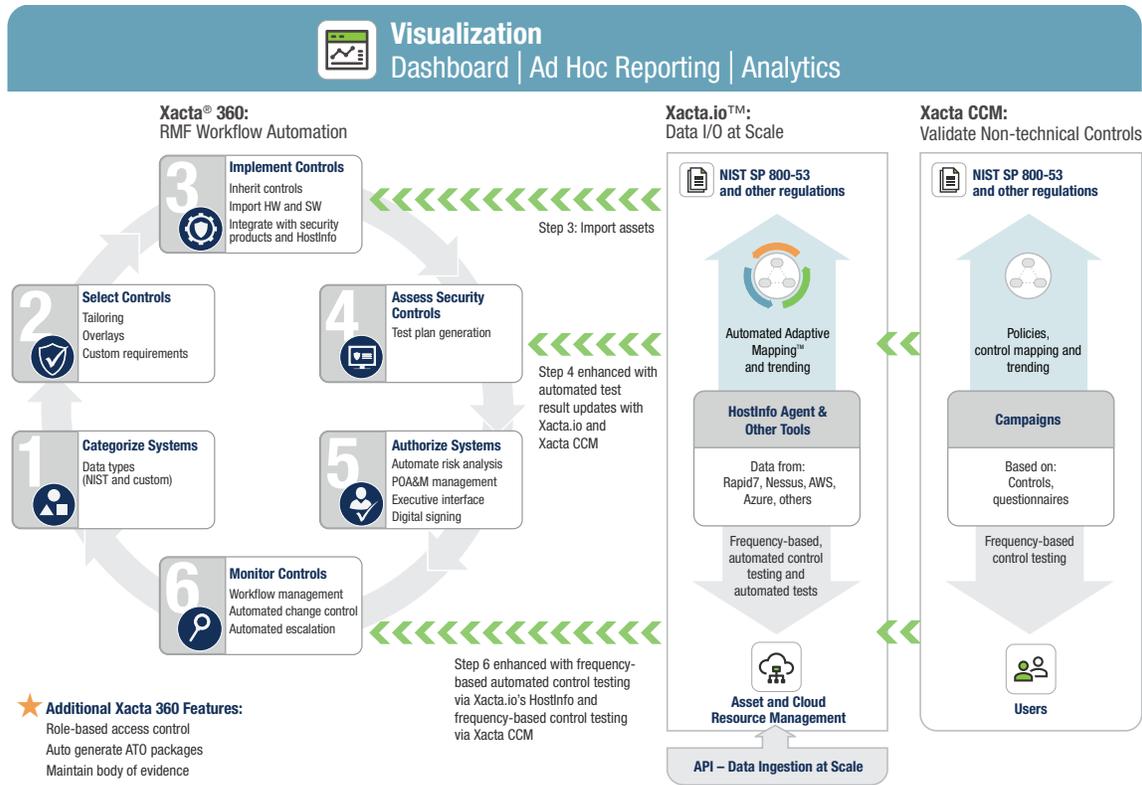## Xacta.io™ Automates Continuous Monitoring for Ongoing Risk Management

Ongoing monitoring of security controls is the ultimate step in the NIST RMF. Xacta.io is the Xacta component that enables you to collect and correlate results from multiple security sources and map them to the relevant controls in support of risk management and continuous monitoring.   Its capabilities include:

- **Adaptive Mapping™ to Connect Vulnerabilities and Related Controls.** Adaptive Mapping automatically detects and plots the points of intersection among vulnerabilities, controls, and assets. It gives security testers and assessors the power to look across multiple security feeds and understand how they influence a variety of controls and requirements for a particular product or system.

- **Automated Testing to Enhance Security Controls Assessments.** Xacta.io leverages the third-party agents your security products currently use, complemented by a secure, lightweight framework for agent-driven host data collection that allows you to do scheduled and ad hoc compliance tests. Results are mapped to controls and auto-fill your test plan, which is then fed back into Xacta 360 for test-plan generation.

- **Frequency-based Testing for Ongoing Controls Monitoring.** Xacta.io supports frequency-based automated controls testing through Xacta HostInfo agents. This is a family of host-specific software used to collect a comprehensive amount of security-relevant configuration information about an asset for compliance assessment. The ability to schedule tests ensures you can monitor your security controls on an ongoing basis in keeping with Step 6 of the RMF.

While everyone wants to follow the RMF, most agencies value an outside perspective on the how. Telos can assist with all aspects of the transition, including business process re-engineering. We're able to help agencies and organizations move to the new risk-based method for managing cybersecurity. We have the understanding, background, and solutions to ensure a smooth, successful transition.

Please contact us to discuss how we can help you with the move to the NIST RMF. Telos solutions and services are available on GSA schedule and a variety of federal contracts.

Visualization
Dashboard │ Ad Hoc Reporting │ Analytics

Xacta® 360: RMF Workflow Automation

3 Implement Controls
Inherit controls
Import HW and SW
Integrate with security products and HostInfo

2 Select Controls
Tailoring
Overlays
Custom requirements

1 Categorize Systems
Data types
(NIST and custom)

4 Assess Security Controls
Test plan generation

5 Authorize Systems
Automate risk analysis
POA&M management
Executive interface
Digital signing

6 Monitor Controls
Workflow management
Automated change control
Automated escalation

★ **Additional Xacta 360 Features:**
Role-based access control
Auto generate ATO packages
Maintain body of evidence

Step 3: Import assets

Step 4 enhanced with automated test result updates with Xacta.io and Xacta CCM

Step 6 enhanced with frequency-based automated control testing via Xacta.io's HostInfo and frequency-based control testing via Xacta CCM

Xacta.io™: Data I/O at Scale

NIST SP 800-53 and other regulations

Automated Adaptive Mapping™ and trending

HostInfo Agent & Other Tools
Data from:
Rapid7, Nessus, AWS, Azure, others

Frequency-based, automated control testing and automated tests

Asset and Cloud Resource Management

API – Data Ingestion at Scale

Xacta CCM: Validate Non-technical Controls

NIST SP 800-53 and other regulations

Policies, control mapping and trending

Campaigns
Based on:
Controls, questionnaires

Frequency-based control testing

Users

Xacta automates the NIST RMF. *The components of the Xacta suite for security risk management work together to automate the A&A process.*