Continuous Monitoring

Integrated services, best practices, and automation tools from Telos Corporation — the leader in federal cybersecurity.

Telos®
Continuous monitoring of information systems has long been a goal of cybersecurity professionals for improving the security of federal networks. Efforts to reach this goal are gaining momentum.

- The Risk Management Framework (NIST Special Publication 800-37 Revision 1, released in February 2010) includes continuous monitoring as the ultimate step in that risk management process and identifies essential elements to a successful organization-wide continuous monitoring program.

- NIST SP-800-137, “Information Security Continuous Monitoring for Federal Information Systems and Organizations,” was released in draft in December 2010 to assist organizations in the development of a continuous monitoring strategy and the implementation of a program that provides visibility into assets, awareness of threats and vulnerabilities, and visibility into the effectiveness of security controls.

- NIST SP-800-39, “Managing Information Security Risk,” was released in March 2011 to expand the focus of information security risk management from the system level to the enterprise level. It includes continuous monitoring processes to ensure that security controls, services, and technologies are operating effectively throughout the system development life cycle.

- The 2011 FISMA compliance metrics from the Department of Homeland Security reflect the need for agencies to continuously monitor more than a dozen different data feeds from IDS/IPS and AV scanners, vulnerability scans, system and application logs, and other sources.

Achieving continuous monitoring requires a balanced combination of processes, people, and technologies to help organizations automatically detect and report vulnerabilities in the IT environment.

These factors make Telos Corporation a logical choice for emerging continuous monitoring programs. We tailor our cybersecurity services and solutions to our customers’ specific technology and business environment – a key requirement for effective continuous monitoring.

Telos works with agencies to help them establish, implement, and maintain a continuous monitoring program in accordance with guidance from Draft NIST SP 800-137:

- Define continuous monitoring strategy;
- Establish measures and metrics;
- Establish monitoring and assessment frequencies;
- Implement a continuous monitoring program;
- Analyze data and report findings;
- Respond with mitigating strategies, or transfer or accept risks; and
- Review and update continuous monitoring strategy and program.
Telos Cybersecurity Services

Telos has provided cybersecurity services to the DoD, the Intelligence Community, federal civilian agencies, and commercial marketplace for more than 20 years. Telos employs over 140 cybersecurity analysts and engineers, most holding major security certifications (CISSP, CISA, CCNA) with clearances up to TS-SCI, allowing us to work at the highest levels of security sensitivity.

Our staff’s professional qualifications, combined with over two decades experience in providing security services, demonstrate our ability to provide world-class security services to our customers. For example:

- Telos cybersecurity engineers have ensured compliance of the Pentagon backbone networks with the governing DoD and NIST security guidelines, protecting thousands of users at dozens of locations in the National Capital Region.

- Telos supports diverse executive branch cybersecurity initiatives for GSA, including continuous monitoring via application and database vulnerability scanning, wireless network assessments, and secure configuration compliance.

- Telos supports member agencies of the Intelligence Community with continuous monitoring policy and strategy development, engineering and tool deployment, and support and operation.

Our services in support of continuous assessment include:

SECURITY POLICY AND OPERATIONAL PROCEDURE DEVELOPMENT. Telos consultants have a wide range of experience in developing, reviewing, and enforcing security policies for many different types of government and commercial agencies. Because our engineers have worked in operational environments as both technicians and security engineers, they are ideally suited to develop continuous monitoring procedures that ensure network and system performance as well as security.

SECURITY ENGINEERING AND ARCHITECTURE DESIGN. Continuous monitoring requires an understanding of a broad variety of information technologies, security requirements, and how they work together. Telos security engineers have experience with security information and event management systems (SIEMs), IDS/IPS and firewalls, enterprise operating systems as well as the application and database layers, and other resources that must be included in a continuous monitoring architectural framework.

OPERATIONAL SECURITY MANAGEMENT. Telos network security and operations personnel have experience monitoring network security 24/7/365 in some of the most security-conscious agencies of the federal government, the intelligence community and Department of Defense, including the Pentagon’s Security Operations Center. Telos personnel function as a team to protect the network from failures, cyber attacks, network misconfigurations, viruses, and other vulnerabilities and threats.
Best-of-breed Approaches and Technologies For Continuous Monitoring

Telos adheres to established IT security processes and frameworks to ensure the continuous monitoring and management of security postures. Our services and solutions reflect the recommendations of the NIST Risk Management Framework; the Continuous Asset Evaluation, Situational Awareness, and Risk Scoring (CAESARS) model for continuous asset evaluation and risk scoring; the emerging FedRAMP requirements for assessing and authorizing cloud computing services and products and others.

**NIST RISK MANAGEMENT FRAMEWORK**

The NIST Risk Management Framework (RMF) laid out in SP 800-37 provides a structured approach to managing risk throughout a system’s life cycle. It identifies the elements essential to a successful organization-wide continuous monitoring program, including:

- Configuration management and change control
- Security impact analyses
- (Ongoing) assessment of system security controls
- Security status monitoring and reporting
- Active involvement of organizational officials in the ongoing management of information system security-related risks

The sixth and final step of the RMF calls for the monitoring of security controls by determining the security impact of system changes, assessing a system’s security controls in accordance with defined strategies, conducting remediation actions when indicated, updating security plans based on the results of continuous monitoring, and reporting and reviewing security status.

The RMF also operates at Tier 3 (system level) of NIST SP 800-39 as well as interacting with Tier 1 (governance level) and Tier 2 (process level) by providing feedback from authorization decisions to the risk executive function and disseminating updated risk information to authorizing officials, common control providers, and information system owners.

**CAESARS: RISK SCORING BEST PRACTICES**

The DHS Federal Network Security Branch issued the CAESARS detailed reference architecture that offers best-practices and an integrated approach with end-to-end processes for:

- Assessing the state of each IT asset under an organization's management
- Determining the gaps between the current state and accepted security baselines
- Expressing in quantitative measures the relative risk of each gap or deviation
- Providing letter grades that reflect the aggregate risk of sites and systems
- Ensuring that the responsibility for every system and site is assigned
- Providing targeted information for security and system managers to use in taking the actions necessary to make changes needed to reduce risk
- Inspiring and encouraging competition among agency managers through measured and recognized improvement

Telos integrates new frameworks and standards into our work as they are available, tailoring each one to our customer’s specific circumstances.

**FEDERAL RISK AND AUTHORIZATION MANAGEMENT PROGRAM (FedRAMP)**

FedRAMP is designed to establish a unified risk management framework for cloud computing. This emerging standard set of controls and defined processes will result in cost savings and help to eliminate the discrepancies among agencies authorization processes by:

- Providing a framework that is compatible with FISMA security requirements and has been vetted by various government agencies and industry
- Offering effective and consistent assessment of cloud services
- Focusing continuous monitoring on near real time data feeds from cloud service providers
- Using the “approve once, use many” concept

Telos integrates new frameworks and standards into our work as they are available, tailoring each one to our customer’s specific circumstances.
**Xacta automation tools to streamline processes for continuous monitoring.**

Human judgment is essential in sound cybersecurity assessment and monitoring. But automation tools can also streamline processes and help eliminate errors and oversights. As NIST SP 800-137 suggests, “Real-time monitoring of implemented technical controls using automated tools can provide an organization with a much more dynamic view of the security state of those controls.”

Telos began automating security-related tasks through its Xacta IA Manager enterprise software offering over a decade ago and continues to support continuous monitoring and related activities with automation capabilities wherever they improve accuracy and efficiency.

---

**Xacta IA Manager: Take control of your risk and compliance posture for continuous monitoring and security risk assessment.**

Xacta IA Manager offers continuous assessment capabilities that enable organizations to track the security state of a wide range of information systems on an ongoing basis and maintain the security authorization for the systems over time. Its elements work together to provide CISOs and other senior leaders with a dynamic view into the current status of security controls.

**Xacta Continuous Assessment** automatically detects changes to the IT environment so you always have situation awareness of potential risks and threats. Its automatic vulnerability update service delivers the right guidance at the right time about what actions to take in response to potential threats.

Its tightly integrated, complementary components include:

**Xacta Asset Manager: Organize your IT asset data as actionable information.** Xacta Asset Manager is the central repository for asset and configuration management information. It automatically imports asset data from systems and enterprise management platforms and offers a central repository to organize your IT asset data as actionable information.

---

**TELOS: A DEEP LEGACY IN CONTINUOUS MONITORING**

Telos Corporation has been an advocate of continuous assessment, monitoring, and enforcement for more than a decade. We first conceived of continuous assessment in 1999 as part of our long-term strategy to make the C&A process more meaningful — less about documentation and paperwork drills, more about understanding risk posture on an ongoing, continuous basis.

Telos introduced its patented continuous assessment functionality in Xacta IA Manager in February 2003. Today our cybersecurity personnel continue to monitor and protect some of the largest networks in the world and continually enhance the capabilities of Xacta IA Manager for today’s continuous monitoring requirements.
Xacta Detect: Manages agent tasking and collects vulnerability and configuration data. Xacta Detect performs discovery scanning and executes data collection scans to aggregate configuration and vulnerability data. It identifies network assets and inventories each hardware component as well as its associated operating system and software applications. Discovery Scans are used to identify network devices that do not have agents.

Xacta HostInfo: Gather the information needed for security assurance. This family of platform-specific executables collects and provides security-relevant configuration information to the Xacta Detect server for assessment. Xacta HostInfo also supports NIST SCAP-validated testing capabilities to determine compliance with FDCC and other XCCDF checklists. HostInfo has the capability to communicate directly with Xacta Detect for fully automated collection of vulnerability and configuration results which are then relayed to Xacta Asset Manager for compliance reporting. HostInfo is supported on Windows, MAC OS X, Solaris, and RedHat Linux.

Xacta Flux: Automate mapping of IT asset scans to the relevant controls. Xacta Flux automates the complex task of mapping scans of IT assets to the relevant standards for security and risk management, such as NIST, DIACAP, ISO, and others. It takes scans from multiple, disparate sources and correlates the individual results on the fly to the corresponding controls. You can then use these results to create reports for analysis and to reveal trending. Xacta Flux accepts configuration and vulnerability data captured from a long list of security tools that assess hosts, application servers, databases, and source code. Configuration and vulnerability data that cannot be captured in an automated fashion can be easily collected using the Xacta Interview Tool, a SCAP OCIL compliant tool.
Other key capabilities of Xacta Continuous Assessment include:

- **Vulnerability correlation** — Correlates vulnerability information from disparate scan sources so cybersecurity personnel can make more informed decisions and plan the appropriate next steps.

- **Remediation planning** — Facilitates the development of remediation plans for individual issues on each asset.

- **Security assessment result mapping** — Enables consistent mapping of results from any security source across an organization or individual business unit.

- **Confidence scoring** — False positive/negative results are tracked to determine confidence ratings of results from all security sources to ensure accurate findings.

- **Trending analysis** — Multiple testing cycles can be analyzed and compared to determine effectiveness of remediation efforts as well as rising areas for concern.

**Contact Telos to begin planning your continuous monitoring program.**

We look forward to applying our cybersecurity capabilities to your continuous monitoring requirements. Please contact us to begin a conversation about how we can help you keep your finger on the pulse of your cybersecurity posture.