WHITEPAPER 2017

THE REAL-TIME ASSURANCE ENGINE

Operationalizing Security and Compliance through Automation

XCELERATE SOLUTIONS

Secure Results. Delivered.

xceleratesolutions.com

TABLE OF CONTENTS

The Xcelerate Real-time Assurance Engine (XRAE) transforms compliance and security from mandates to institutionalized, value-based practices that effectively manage risk, increase security, and deliver business value. XRAE is based on our extensive experience transitioning customers to the National Institute of Standards and Technology (NIST) Risk Management Framework SP 800-53 (RMF); proactively monitoring their enterprise systems for cyber risks, threats and vulnerabilities; and automating the generation of compliance artifacts. This paper provides an in-depth view of how XRAE works and the value that it brings to your organization.

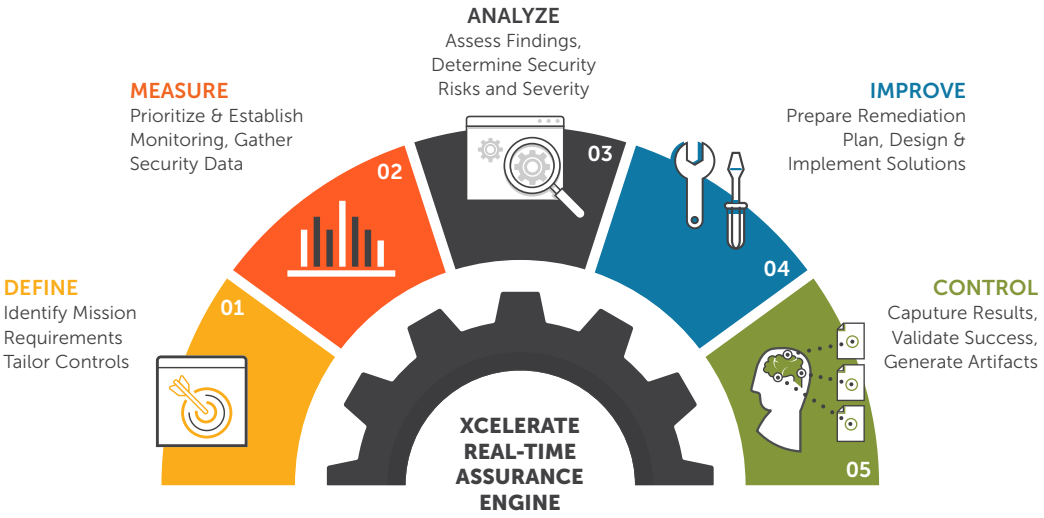
XRAE is the result of applying our Lean Six Sigma mastery to the unique cybersecurity challenges of the United States Government.

CONCEPT

With Department of Defense (DoD) Instruction 8510.01, the Chief Information Officer directed the establishment and use of RMF for enterprise-wide cybersecurity risk management. RMF provides a structure for categorization of systems and the subsequent selection, implementation, assessment, authorization, and monitoring of security controls, but adopters have found that it can quickly become cumbersome if not augmented by a vigilant and automated sustainment approach. Furthermore, the actual implementation of RMF is open to each organization to address in alignment with their specific mission and profile.

A proactive, continuous, and automated model for enterprise cyber security is required to stay safe and productive in today's dynamic digital landscape. With shrinking budgets and rapid shifts in mission priorities, keeping up with vulnerability alerts is a significant challenge, and implementing an active approach toward threat monitoring even more so.

Compound these challenges with the need for delivery of new or modernized capabilities, and you may find yourself in a frustrating environment where security is viewed as an impediment to delivery.



BENEFITS

There are four key benefits that we are able to deliver to any enterprise through XRAE's effective and automated security and compliance methodology:

1. EFFICIENCY, brought by the automation of routine compliance tasks and tailored to the specific documentation and deliverables required by your enterprise for continued Assessment & Authorization (A&A) and Authority to Operate (ATO). We give you back your time to focus on delivering improvements to the satisfaction of your users and stakeholders.

2. SECURITY through a streamlined and disciplined approach to reducing operational risk, resolving Plan Of Action & Milestones (POA&M) items, and identifying vulnerabilities in your network. We base our actions on the robust expectations of Government cybersecurity requirements—the RMF, Defense Information Systems Agency (DISA) Security Reference Guides and Security Technical Implementation Guides (STIG), and DoD Computer Emergency Response Team Information Assurance Vulnerability Alerts (IAVA)—and our intimate knowledge of cybersecurity best practices for systems, services, and technologies. In addition to addressing all compliance requirements and controls inherited by or mandated for your organization, we safeguard your networks against vulnerabilities that have not yet made their way through the Government's process.

3. READINESS for ongoing A&A activities, Cyber Command Readiness Inspections (CCRI), and audits through the real-time and continuous generation of tailored and template-based compliance artifacts. We leverage the expertise gained and reuse templates developed from our assessment of over 550 enterprise systems for our Government customers, during which we identified bottlenecks in ATO status, designed and recommended corrective actions, and championed the implementation of improvements. By applying our model, we ensure your mission's continued compliance with POA&M item identification and resolution and generate reports that satisfy the requirements of oversight agencies for fast and low risk review processes.

4. KNOWLEDGE to enhance enterprise decision-making, rapid prioritization of remediation activities, and effective reduction in risk. We streamline this business intelligence by establishing lexicons of common terminology to baseline understanding and facilitate cybersecurity-related communication across the enterprise. Our dedication to accountability and transparency ensures your ability to track risk mitigation activities and results in real-time, enhanced through our use of tools that automatically update enterprise network and system views.

An innovative approach to compliant and secure enterprise risk management for our customers that actually frees time for development and sustainment of systems and services.

RISK MANAGEMENT OVER RISK AVOIDANCE

We believe that risk avoidance is not a feasible approach given the need to balance the benefits of sharing information and intelligence with the ever-present set of nefarious actors that are eager to get their hands on it. Risk management, on the other hand, acknowledges that the likelihood of cybersecurity risks being realized is never zero, and instead prioritizes activities that continually reduce those chances for the highest impact targets.

XRAE is designed with this model in mind, taking an agile approach to implementing continuous cybersecurity posture improvement for your enterprise. In this model, you will realize reductions in risk in short (e.g., 2-3 week) increments—including design, development, and testing—rather than after months or years of wholesale system re-architecture and re-engineering.

Our Cybersecurity experts have supported the DoD across RMF functional areas and roles, including Authorizing Official Designated Representative; Security Control Assessor and Test Engineer; and Information Systems Security Officer, Manager, and Engineer.

For the Department of Homeland Security, our Black Belts have provided coaching, mentoring, and implementation of enterprise process improvement projects resulting in $70M+ in cost avoidance and $200M+ in Government-projected savings.

THE INTERSECTION OF LEAN SIX SIGMA AND CYBERSECURITY

Xcelerate Solutions' (Xcelerate) Master Black Belts have extensive experience both process improvement projects built around Lean Six Sigma, and our cybersecurity subject matter experts have the breadth and depth of experience to know what it takes deliver secure and resilient personnel, systems and infrastructure. We have tailored the proven Six Sigma Define-Measure-Analyze-Improve-Control (DMAIC) process to improve the cybersecurity posture of our U.S. Government customers.

1. DEFINE

Identify Mission Requirements / Tailor Controls

Leveraging our automated tooling, we continuously perform quick assessments of your enterprise and evaluate the "lane" into which your organization falls to automatically determine what documentation is required and/or provides significant enterprise security value. With this information in hand, we identify the specific controls that must be applied to your systems.

2. MEASURE

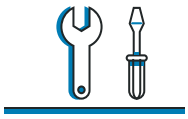
Prioritize & Establish Monitoring, Gather Security Data

Based on the definition of your systems and services, we leverage our expertise in automated tools and technologies to identify monitoring solutions for the highest priority aspects of your environment. Our recommendations on priority may be based on mandates and/or risk to your organization, and we provide you with all the information you need to effectively make decisions on approval and approach. We then immediately begin gathering security data for analysis.

3. ANALYZE

Assess Findings, Determine Security Risks & Severity

With real-time security data (logs, configurations, etc.) in hand, we then look for any discrepancies with the expected configuration (as identified in Define). We apply an automate-everything mentality to our work to ensure that we do not need to perform repetitive tasks to deterime cybersecurity risks and severity. We can further augment this analysis through our innovative Cyber Hunting capabilities, seeking out and stopping advanced and insider threats.



4. IMPROVE

Prepare Remediation Plan, Design & Implement Solutions

In this step, we take the results of analysis and build agile remediation plans, designing, implementing, and testing solutions in an itereative and incremental manner to reduce operational risk. We leverage our Project, Program & Portfolio Management expertise to successfully bring each improvement initiative to fruition in a streamlined and transparent manner.

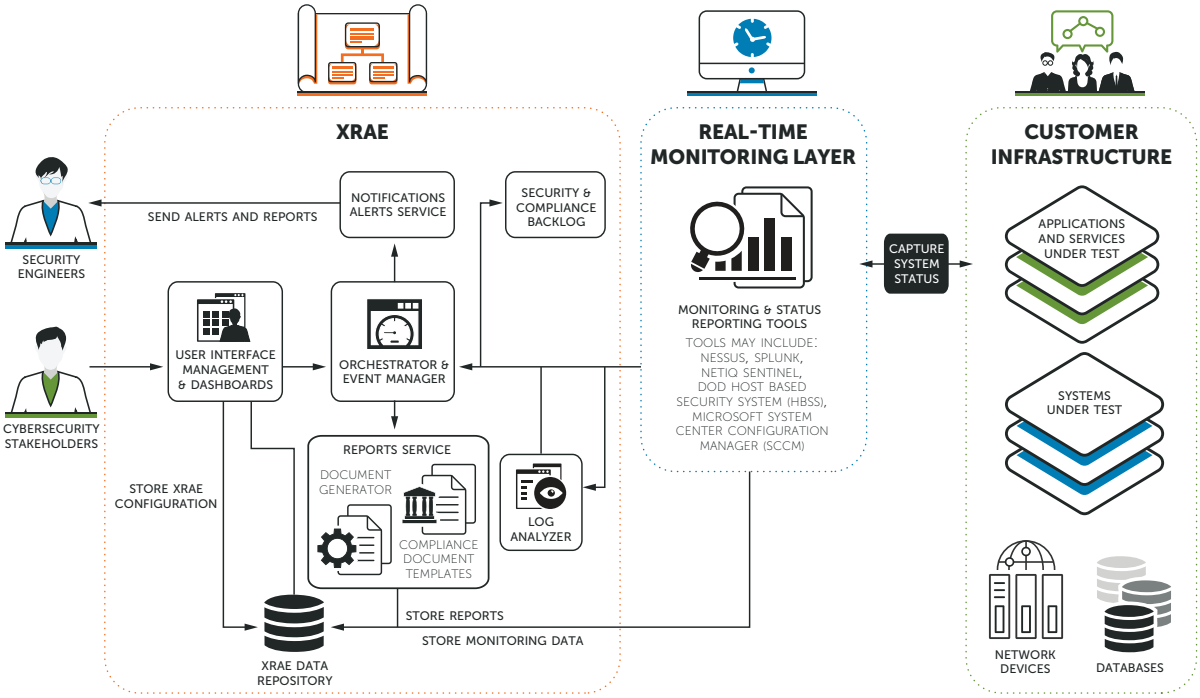
5. CONTROL

Capture Results, Validate Success, Generate Artifacts

With security posture and process improvement solutions deployed, we review the ongoing metrics and measurements to ensure that the results are what we we intended, building automated alerts and updates should controls be compromised through ongoing operations. We are also now able to automatically update risk posture documents, recommend closing of POA&M items, and generate the artifacts necessary to achieve and maintain your ATO.

ARCHITECTURE

The foundational layer of XRAE is responsible for ingesting monitoring data, analyzing that information for continued compliance, creating backlog items (tasks) for security incident management, generating notifications and alerts for the incident response team, and producing reports and compliance artifacts from templates for stakeholders. The timing of all these activities is handled by the Orchestrator as it reacts to events from users and other services in XRAE. These architectural components are all modular, enabling XRAE to be deployed in an incremental manner, rapidly bringing individual capabilities to bear based on the priorities of our customers.



Between the customer's infrastructure systems and services and XRAE itself are tools—determined as a result of the Measure phase—that are responsible for monitoring the production environment and applying or ensuring configuration. As data is captured, it is sent to analysis services for real-time processing, and alerts are generated whenever abnormal findings are detected. The actual tasks to remediate these findings are tracked in a backlog that our security engineers use to manage their work. Furthermore, the reports service, based on the results from the monitoring tools and using standardized templates, generates updated compliance documentation. The outcome is a shift in your focus from creating compliance documentation to simply reviewing prior to submission.

APPLICATIONS

We are ready to apply XRAE to improve risk management and posture in any cyber enterprise. The samples below illustrate just some of what Xcelerate can deliver in support of your mission through the operationalization and automation of security and compliance.

COMPLIANCE IN THE CLOUD A program is performing a migration of services to the cloud from their legacy infrastructure. With this new architecture and a partnership with a cloud service provider, the program needs to identify what security controls they have direct responsibility and for which they depend on the provider, implement those controls, and monitor their systems to ensure continuous compliance. Our unified team of cloud architects and cybersecurity professionals apply XRAE to the program to define appropriate controls, measure the new virtual infrastructure, analyze discrepancies, define and implement an improvement plan, and create automated jobs that provide continual validation of the environment. Furthermore, by leveraging XRAE's document generation capabilities and custom-tailored templates, we are able to create A&A artifacts without significantly occupying the time of the program's valuable system engineers.

Operationalize and automate security and compliance in your environment.

THE NEVER-ENDING LIST OF POA&M ITEMS An agency has transitioned to using the RMF and now has a lengthy POA&M to address all the issues that were identified as part of the A&A process. They bring in XRAE to help balance the demands of this challenge while still delivering new and updated services to their customers in support of their critical mission. Xcelerate experts assess the POA&M and the agency's enterprise systems, identifies measurement techniques to evaluate successful item resolutions, build plans to iteratively and incrementally address issues, and applies automation to regenerate compliance artifacts as every change is applied. The result is a balanced approach to addressing the needs of security and delivery, ensuring that the systems retain their ATO and provide the capabilities that their customers need.

REGULAR INTERRUPTION OF PRODUCTION SERVICES FROM SECURITY PATCHES An organization receives IAVAs and follows the guidance in STIGs, but all too often the actions they take cause downtime or unacceptable performance degradation of critical production systems and services. Xcelerate applies XRAE to provide a tighter integration between the security and testing teams, implements monitoring tools that provide immediate alerts on potential and realized production issues, and institutes its framework for designed, tested, and controlled change management. With all security patching now performed only when there is a true need and with appropriate testing, the organization notices an immediate improvement in reliability and uptime.

Furthermore, in rare situations that their mission critical activities are in conflict with guidance, they have the information they need for effective justification of waivers and the knowledge of the effects on their risk profile. Xcelerate also found that by implementing our Automated Test Framework—a proven means of automating functional, regression, and performance testing—the activities of the organization's testing team could be streamlined to provide confidence in the success and seamlessness of each patch activity.

XCELERATE SOLUTIONS

Secure Results.
Delivered.

FOR MORE INFORMATION ON OUR REAL-TIME ASSURANCE ENGINE CONTACT:

eti@xceleratesolutions.com

ABOUT XCELERATE SOLUTIONS

We exist to create innovative solutions that deliver results, manage risk from individuals to systems, and *xcelerate* time to value. Across our three practices — Enterprise Technology & Innovation; Project, Program & Portfolio Management; and Enterprise Process Management — we optimize efficiency and effectiveness and enhance the security and resilience of America's personnel, physical and cyber infrastructure.

PHONE 703.462.1500 **SOCIAL** @XLR8Solutions xceleratesolutions.com
HEADQUARTERS 8405 Greensboro Drive, Suite 930 McLean, VA 22102

afaq ISO 9001 Quality AFNOR CERTIFICATION

CMMI SVC /3 SM Exp. 2018-10-09 / Appraisal #25322

afaq ISO 27001 Information Security AFNOR CERTIFICATION