Protect government Web assets and support regulatory compliance

Rational. software

Helping government agencies minimize Web site security risks, improve compliance and increase efficiency

IBM Rational software solutions for Web application security and Web site compliance

Highlights

- ***Helps government agencies comply with standards and regulations from the Office of Management and Budget (OMB), the Office of the Secretary of Defense (OSD) and the Intelligence Community (IC)***
- ***Helps automate Web risk management processes to increase IT productivity***
- ***Helps agencies improve site security and privacy by analyzing Web sites for vulnerabilities***
- ***Helps agencies enhance site usability and accessibility by scanning for hundreds of common issues***
- ***Integrates with existing processes and organizational frameworks to help agencies optimize for greater efficiency and effectiveness***

Supporting compliance with Web risk management standards and mandates

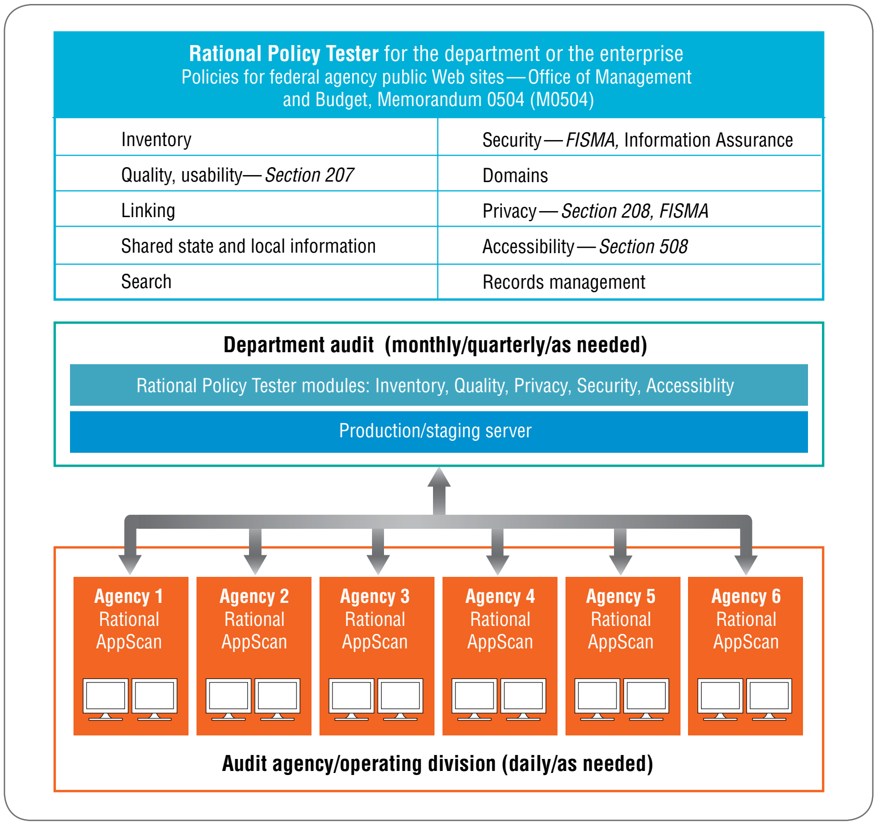
Government agencies must comply with a long list of regulations and standards for managing security and performance risk in physical and network IT operations. But risks also reside on agency Web sites—according to Gartner, 75 percent of all hacking attempts occur at the Web application layer. To achieve compliance requirements, agencies face several challenges—establishing processes to identify risk in Web operations; monitoring, remediating and measuring those risks; and creating a method of reporting to meet government standards.

IBM Rational® AppScan® and IBM Rational Policy Tester software together can provide a highly comprehensive Web risk management platform. These applications automate the process of scanning, analyzing and reporting Web security, privacy, usability, accessibility and compliance issues across agency Web properties.

Your agency can use Rational AppScan and Rational Policy Tester to implement processes that help streamline risk management and improve compliance with a number of government requirements, including those demanded by:

- *Federal Information Security Management Act (FISMA).*
- *National Institute of Standards and Technology (NIST).*
- *Security Content Automation Protocol (SCAP).*
- *Department of Defense (DoD) Information Assurance Certification and Accreditation Process (DIACAP).*
- *Director of Central Intelligence Directives (DCID).*
- *Operations Security (OPSEC).*
- *Section 208 privacy initiatives.*
- *Section 207 quality initiatives.*
- *Section 508 accessibility initiatives.*

Compliance with these regulations enables agencies to follow the President's Management Agenda (PMA), which was launched in 2001 as a strategy to improve federal government



Rational Policy Tester for the department or the enterprise
Policies for federal agency public Web sites—Office of Management and Budget, Memorandum 0504 (M0504)

Inventory	Security—*FISMA,* Information Assurance
Quality, usability—*Section 207*	Domains
Linking	Privacy—*Section 208, FISMA*
Shared state and local information	Accessibility—*Section 508*
Search	Records management

Department audit (monthly/quarterly/as needed)

Rational Policy Tester modules: Inventory, Quality, Privacy, Security, Accessiblity

Production/staging server

Agency 1 Rational AppScan

Agency 2 Rational AppScan

Agency 3 Rational AppScan

Agency 4 Rational AppScan

Agency 5 Rational AppScan

Agency 6 Rational AppScan

Audit agency/operating division (daily/as needed)

Figure 1: Rational AppScan and Rational Policy Tester software helps agencies address compliance requirements across several areas, including security, privacy, quality, inventory and accessibility.

management and performance, with an emphasis on providing better services to citizens and warfighters through the use of information technology.

Enable OMB compliance monitoring

Rational AppScan and Rational Policy Tester modules for quality, privacy, security and accessibility analyze and map audit results specifically to OMB regulations, which are based on Interagency Committee on Government Information (ICGI) best practices.

By reporting on OMB Web compliance risks, agencies are better able to mitigate Web risk, achieve their missions and fulfill the requirements of the PMA.

Enhance Web application security and privacy

The Security module in Rational AppScan analyzes Web sites for vulnerabilities and helps reduce data theft, breaches in user identity, service interruptions and Web site defacement. With the Privacy module in Rational Policy Tester, users can generate Web privacy reports that identify issues such as missing privacy statements, insecure data collection forms, cookie/beacon presence, Platform for Privacy Preferences (P3P) implementation and third-party links to inappropriate or undesirable sites.

Improve user experience and Web content

The Quality module in Rational Policy Tester scans Web properties for usability issues, including:

- *Broken or missing links.*
- *Slow-loading pages.*
- *Poor searchability.*
- *Browser capability and usability errors.*
- *Incorrect page layout and outdated standard fonts or logos.*

Enable Web accessibility

With the Accessibility/Section 508 module in Rational Policy Tester, users can scan Web properties for more than 170 comprehensive Web accessibility checks. These checks help automate compliance with the Section 508 government accessibility standard, Web Content Accessibility Guidelines (WCAG) for the World Wide Web Consortium (W3C) and other international guidelines.

Understand the Web environment

The Inventory module in Rational Policy Tester conducts an inventory of your Web site and provides an excellent graphical depiction of the entire site—Web servers, technologies in use and the organizational policies and standards in place. With this information, executives have a clear understanding of the assets they have and are better equipped to make business decisions.

Simplifying analysis and reporting with dashboards

Rational AppScan and Rational Policy Tester provide dashboards that help ease the process of OMB reporting and contribute to the implementation of the PMA by helping agencies to:

- *Provide Web risk measurement and management reporting for budget-to-performance integration.*
- *Enable all employees to make quick decisions with actionable information in detailed audit reports and recommendations for mitigating risk.*
- *Improve Web content quality control and efficiency by identifying issues in the development phase of the software development lifecycle (SDLC), rather than in the production phase.*
- *Meet requirements of competitive sourcing with the most comprehensive Web risk management solution.*
- *Improve return on investment (ROI), capital investment and cost containment.*
- *Strengthen e-government initiatives to be more secure, private, usable and accessible.*

Integrating processes with the existing government organizational framework

Rational AppScan and Rational Policy Tester both help agencies incorporate risk mitigation, usability, accessibility, privacy and security processes in the SDLC by leveraging the principles of the Federal Enterprise Architecture (FEA). The result is information systems that meet government requirements, and a set of processes that map to the way your agency works, not the other way around.

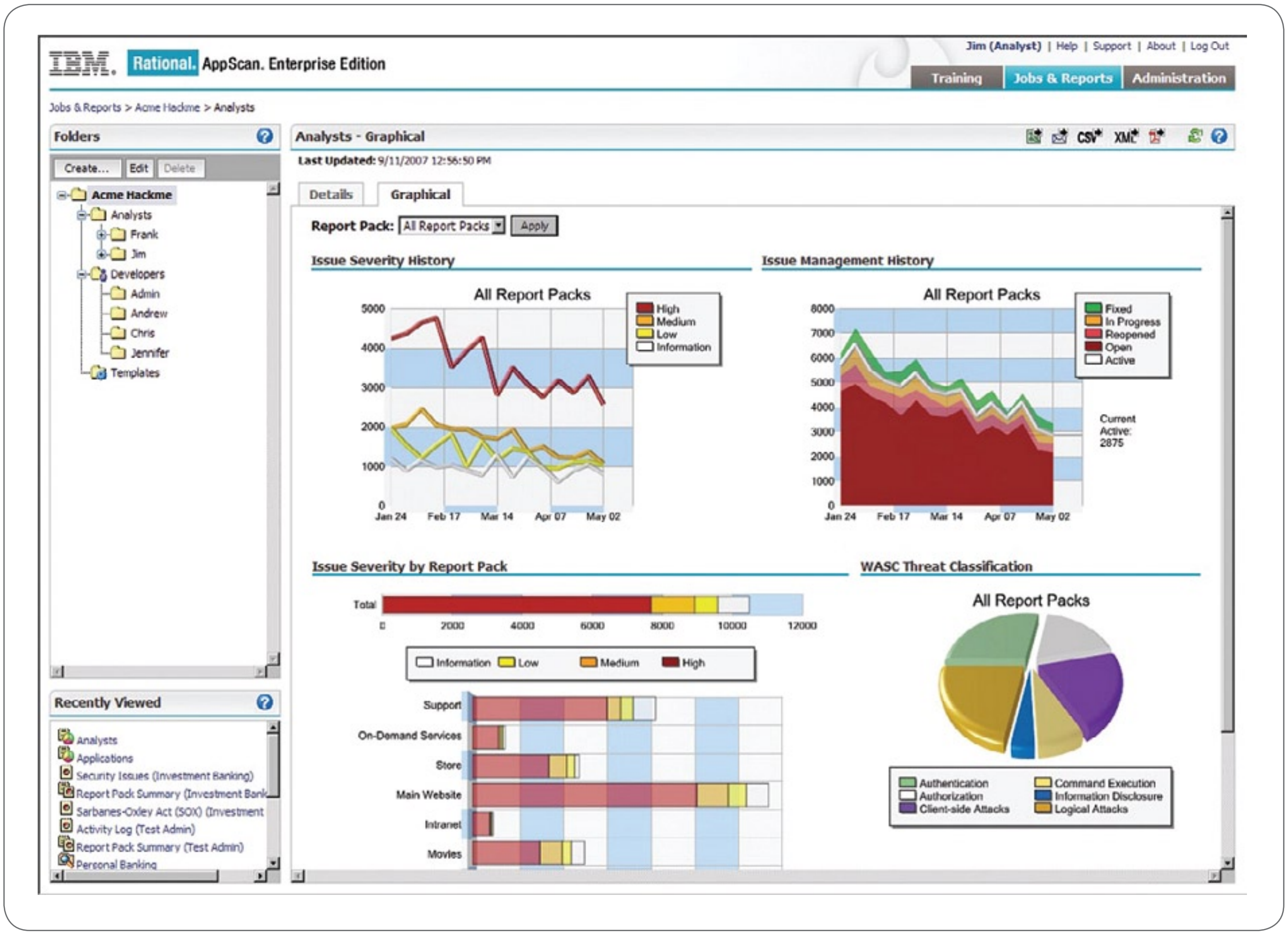
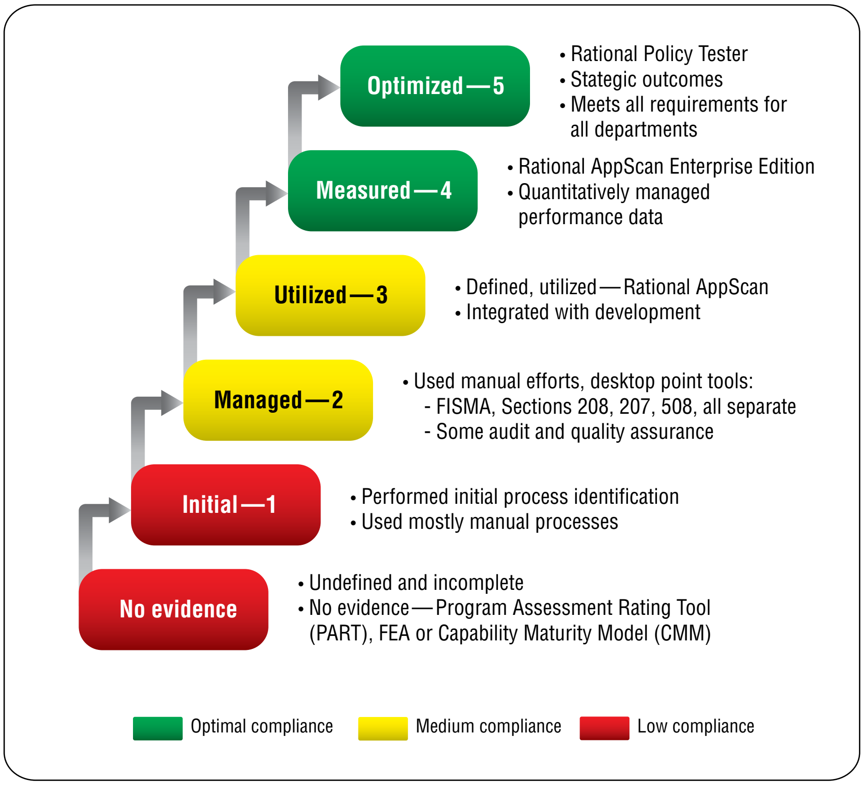


Figure 2: IBM Rational Policy Tester executive dashboard

Which phase are you in?



Optimized — 5
- Rational Policy Tester
- Stategic outcomes
- Meets all requirements for all departments

Measured — 4
- Rational AppScan Enterprise Edition
- Quantitatively managed performance data

Utilized — 3
- Defined, utilized — Rational AppScan
- Integrated with development

Managed — 2
- Used manual efforts, desktop point tools:
  - FISMA, Sections 208, 207, 508, all separate
  - Some audit and quality assurance

Initial — 1
- Performed initial process identification
- Used mostly manual processes

No evidence
- Undefined and incomplete
- No evidence — Program Assessment Rating Tool (PART), FEA or Capability Maturity Model (CMM)

🟩 Optimal compliance 🟨 Medium compliance 🟥 Low compliance

Figure 3: This graphic demonstrates how you can leverage Rational AppScan and Rational Policy Tester modules to increase levels of optimization within your department. By adding the technology to your SDLC and measuring results, you can achieve strategic outcomes. These applications can help your agency go from red level (low compliance), through yellow level (medium compliance) to green level (optimal compliance).

For more information

To learn more about IBM Rational Policy Tester and IBM Rational AppScan software and how they can support agencies in their efforts to comply with regulatory mandates, visit:

ibm.com/software/awdtools/appscan/

ibm.com/software/awdtools/tester/policy/

To view a demo about Watchfire, which IBM acquired in July 2007 and incorporated into the Rational product family, visit:

http://www.watchfire.com/products/Webxm/Webxmgovdemo.aspx

IBM Corporation
Software Group
Route 100
Somers, NY, 10589
U.S.A.

Produced in the United States of America
September 2008
All Rights Reserved

The information contained in this documentation is provided for informational purposes only. While efforts were made to verify the completeness and accuracy of the information contained in this documentation, it is provided "as is" without warranty of any kind, express or implied. In addition, this information is based on IBM's current product plans and strategy, which are subject to change by IBM without notice. IBM shall not be responsible for any damages arising out of the use of, or otherwise related to, this documentation or any other documentation. Nothing contained in this documentation is intended to, nor shall have the effect of, creating any warranties or representations from IBM (or its suppliers or licensors), or altering the terms and conditions of the applicable license agreement governing the use of IBM software.

IBM customers are responsible for ensuring their own compliance with legal requirements. It is the customer's sole responsibility to obtain advice of competent legal counsel as to the identification and interpretation of any relevant laws and regulatory requirements that may affect the customer's business and any actions the customer may need to take to comply with such laws.