

Vanguard inCompliance™

In today's high-profile data security environment, businesses, financial institutions and government agencies spend time, money and effort in creating security policies that represent the ideals and objectives of their organization. Security administrators, auditors, legal representatives and management create these pertinent security policies. Too often, the policies are shelved in a three-ring binder and do little more than collect dust.



The Power of Vanguard inCompliance

Vanguard inCompliance is capable of performing millions of critical compliancy checks to guarantee adherence to IBM RACF® best practices. When a compliance check is run, inCompliance detects high exposure changes or an exception to policy standards or rules. Findings are reported interactively at summary levels to satisfy manager and auditor needs down to item-level detail for remediation purposes. inCompliance provides an immediate overview of the entire RACF environment with just one or two mouse clicks from a web browser. Just as easily, you can also narrow the scope of compliance checking to include just the data that must be covered by SOX, HIPAA or other regulatory compliance reports

Highlights

- Identifies high-risk situations and/or potential compliance violations.
- Provides continuous "self-audits" that prevent negative external or internal audit findings.
- Detects and reports high exposure and exceptions to security policy standards or rules.
- Can create a security audit that covers your SOX data for an instant compliance audit report.
- Does the same thing for HIPAA, GLBA and many other regulatory reports.

Legislative Pressures For Compliance

Due to the mandate for regulatory compliance as a result of Sarbanes-Oxley, GLB, HIPAA and other legislation, the need for robust reporting tools is more critical than ever before. Organizations are under tremendous pressure to demonstrate accurate reporting with an unprecedented level of granularity. Furthermore, senior executives are now accountable for accurate reporting and companies run substantial risks to the corporate image and to the bottom line. With this introduction of required compliance regulations, implementing an easy-to-use tool that offers the necessary reporting capabilities is more important than ever before.

Benefits of inCompliance

Vanguard inCompliance performs millions of compliance checks in seconds, with just a few mouse clicks. Some of the benefits of implementing inCompliance include:

- Receive an instant overview of an organization's entire Security Server™ (RACF)
- Allows detailed view of any compliancy check

Vanguard inCompliance™
Continuous Audits Verifying System Compliance

- Recommends corrective actions where appropriate
- Encourages authorized users and IT auditors to quickly analyze and identify essential policy standards and rules online through scrollable web pages
- Provides a step-to-step RACF web-based guideline, including demonstrations of all compliance checks.

What inCompliance Does

Vanguard inCompliance automatically performs over 200 critical checks to ensure adherence to (and compliance with) RACF best practices.

It provides an instant overview of the entire RACF environment with just one or two mouse clicks from a web browser. An additional mouse-click permits a “drill-down” to a Detail View of a compliance check. The administrator can immediately identify high-risk changes and potential violations.

With its sophisticated yet easy-to-use web interface, inCompliance allows a user to quickly review the security analysis results of multiple systems. Using an intuitive drill-down sequence, a user can navigate from the initial notation of how a system scored to details of the review.

Adapting Technology to People

Vanguard inCompliance reinstates the user as the driving force in technology. inCompliance allows the user to establish security parameters and thresholds germane to the security policies of that particular business. It fits the technology to the business – and not vice versa. inCompliance detects high-exposure changes or exceptions to a security policy, notifies a designated administrator and prevents negative audit findings through continuous self-audits. It tells the administrator, sitting at one console, what he or she needs to know about a single system or multiple systems, provides demonstrations and actions taken during all compliance checks, and suggests actions to correct deficient areas. It represents the future of information technology.

For More Information

To learn more about the features and benefits of Vanguard enterprise security software solutions, visit www.go2vanguard.com.

Security Management Solutions:
 Vanguard Administrator
 Vanguard Advisor
 Vanguard SecurityCenter

Audit and Compliance Solutions:
 Vanguard Analyzer
 Vanguard inCompliance
 Vanguard Enforcer
 Vanguard Policy Manager

Access Management Solutions:
 Vanguard Authenticator
 Vanguard ez/SignOn
 Vanguard ez/Token
 Vanguard Tokenless Authentication
 Vanguard ez/Integrator
 Vanguard PasswordReset

Intrusion Detection Solutions:
 Vanguard Enforcer

©2008 Vanguard Integrity Professionals All other copyrights, trademarks and/or service marks are the property of their respective owners.



1. A adjust tolerance and compliance settings to requirements.

2. Run the compliance checks and view the results.

Category	Compliant	Exclusions	Not	Reviewed	Compliant	Tolerance
User: General	160	0	100%	160	0	Zero
User: Concepts	247	0	98%	252	5	24
User: TSO Segment	23	0	26%	88	65	20
User: DMV Segment	45	0	87%	52	7	22
Group: General	51	0	43%	118	67	20
			48%	252	130	18
			50%	10	5	12
			54%	202	93	10
			99%	82	1	10
			9%	187	176	11
			100%	432	1	4
			71%	28	9	4
			41%	44	26	2
			20%			0
			100%			0

SmartAssist

Check: Percentage of Dataset Profile Standard Permits That Are Users

Issues: Generally the better organized your RACF database is, the easier it is to administrate, maintain and report on. Using user permits instead of groups often adds overhead and is not organizationally advantageous.

Actions: Where possible, convert the user permits to group permits. It is highly recommended to of user permits.

3. Follow the SmartAssist directions to fix the non-compliant events.

4. Consider this your "Compliance Report Card"