Security and Risk Management Strategies

In-Depth Research Report

Security Compliance Orchestration: A Market Emerges Out of the IT-GRC Fog

Version: 2.0, Aug 08, 2008

AUTHOR(S):

Bob Blakley
(bblakley@burtongroup.com)

Additional Input:

Trent Henry

TECHNOLOGY THREAD:

Risk Management

Conclusion

Security compliance orchestration combines three activities: risk assessment, control management, and evidence generation. These activities must be performed by many people in most organizations, but the chief information officer (CIO) and chief information security officer (CISO) coordinate the activities. Security compliance orchestration solutions are maturing and can deliver real value. The so-called "IT-GRC" market is likely to consolidate around security compliance orchestration solutions, and then to integrate vertically by marrying these solutions to financial and organizational GRC solutions catering to the executive suite and to more specialized risk and controls management tools in the trenches of business IT departments.

BURTON GROUP 7090 Union Park Center · Suite 200 · Midvale, Utah 84047 P 801.566.2880 F 801.566.3611 www.burtongroup.com

Publishing Information

Burton Group is a research and consulting firm specializing in network and applications infrastructure technologies. Burton works to catalyze change and progress in the network computing industry through interaction with leading vendors and users. Publication headquarters, marketing, and sales offices are located at:

Burton Group
7090 Union Park Center, Suite 200
Midvale, Utah USA 84047-4169
Phone: +1.801.566.2880
Fax: +1.801.566.3611
Toll free in the USA: 800.824.9924
Internet: info@burtongroup.com; www.burtongroup.com

Table Of Contents

Synopsis

For many security teams, the process of compliance management has been frustrating and expensive. Often, their goal is to install additional technical controls (e.g., a sprinkle of encryption, snip of additional firewalls, or dash of intrusion detection), add some vendor-supplied reporting, and cross their fingers when the auditor arrives. The problem is that security specialists find themselves adding costly new controls for each audit, and they have tremendous difficulty assessing whether controls are operating effectively. In addition, it's difficult to understand the impact that new compliance or contract requirements have on already-deployed security controls. But perhaps the most worrisome result is that security teams generally overlook critical elements of security compliance, including business risk, organizational security policy and non-technology controls assessment, and comprehensive collection of evidence.

To orchestrate security compliance—that is, to identify important risks, choose appropriate controls, map them to appropriate objectives and standards, and monitor compliance—organizations must address both process and policy. Security compliance orchestration tools need to focus on security, compliance, and orchestration.

Increasingly, security compliance orchestration tools address all three areas: risk assessment, evidence collection, and orchestration of workflow. They bring together risk assessment, policy management, and monitoring/feedback. Many so-called “IT-GRC” tools exploit vulnerability management and infrastructure assessment to perform some level of technical monitoring; and they increasingly report instances of failure to comply with standards. But most Burton Group clients report that more than 50% of their security controls are not technological, and in these cases a technical policy-management tool that can do just a bit of reporting on the Sarbanes-Oxley Act (SOX) or the Health Insurance Portability and Accountability Act (HIPAA) will not be adequate. The proliferation of controls in this fragmented environment creates large costs and makes it very difficult to assess the real risk status of the organization. Security compliance orchestration tools address these problems by binding together controls, policies, and assessment capabilities in both technical and nontechnical arenas.

Analysis

Compliance. It's a word that has considerable weight for today's security team. It generates a tremendous amount of spending and effort across many areas of an organization, but information protection is crucial in a vast array of regulatory and contractual mandates; as a result, the security team must remain vigilant.

The problems with security compliance are many. First and foremost is that security isn't the only compliance perspective: issues such as corporate governance, manufacturing tolerances, workplace safety, pay-rate requirements, and so forth are all part of the regulatory landscape for various modern enterprises. However, the audience of this report is the security practitioner; therefore, the report focuses on security compliance. And the problems of security compliance are daunting enough:

- How can security experts relate compliance requirements to organizational policies and actual protective controls?
- What is the best way to assess the effectiveness of technological control elements, such as perimeter layers, identity and access infrastructure, content control, and so forth?
- How can security teams assess the effectiveness of the huge number of controls outside the technological realm in a scalable way?
- How can organizational policy be managed over time, communicated to employees, and tested for acknowledgment and awareness?
- What is a good way to report and track compliance activity—and is it possible to monitor continuously?
- How can an organization adjust quickly to changing standards and regulations?
- How can security professionals respond to dozens or even hundreds of assessments and audits without crippling the enterprise's ability to perform its most important job duties?

One approach to comprehensive security compliance is to contract third parties to help with many of the issues above. But the results are not always heartening. For example, one financial-services company paid more than $8 million to a large audit firm for a Sarbanes-Oxley Act (SOX) assessment in effort to soothe some of the pains listed above. Shortly after the assessment, one of the financial firm's executives asked, “How will we do on Gramm-Leach-Bliley Act (GLBA) requirements?” The auditing firm's answer? “We'd be happy to quote you the price for assessing that. . . .” Needless to say, companies are trying to find more automated and repeatable solutions.

However, security compliance orchestration is not a product—it's a process. Improving the process may take multiple tools, and several different product categories are trying to provide solutions that automate the process as best as possible. These different product categories have recently been lumped together into a confusing mess called “IT-GRC.” Burton Group advises customers to avoid talking about “GRC” in any form, as the term is so vague as to be meaningless. “IT-GRC” as a term is actively detrimental to both vendors and customers. It is used to refer to offerings from organizations as diverse as Paisley and OpenPages (who provide executive-level compliance solutions) on the one hand and Aveksa and SailPoint Technologies (who provide detailed entitlements review, attestation, and personnel threat assessment solutions) on the other hand, with security compliance orchestration vendors like those detailed in this report in the middle. As a market category, “IT-GRC” therefore does not describe a consistent set of functions and is applied to vendors that do not compete against one another and that indeed in many cases complement each other. The vendors Burton Group describes as providers of “security compliance orchestration” are often labeled “IT-GRC” vendors, but, unlike “IT-GRC,” security compliance orchestration actually means something and can be applied to a set of vendors whose products have broadly comparable functions.

As noted in the Synopsis, security compliance orchestration tools focus (not surprisingly) on security, compliance, and orchestration.

Focusing on security means providing effective risk assessment and tools. Focusing on orchestration means providing support for assessment, remediation, and reporting workflows. And focusing on compliance means generating and storing comprehensive evidence to document the operation of those workflows.

The focus of risk tools is selection and self-assessment of risk and controls gaps (through user surveys) vis-à-vis major compliance regulations and standards. Risk-tool strengths typically include a broad knowledgebase (i.e., strong mappings of control frameworks to typical controls and assessment questions) and efficient workflow (delegated surveys to pertinent staff across the organization). Their main weakness is minimal ability to automate testing of controls in the technology infrastructure.

The focus of evidence tools is the development, storage, and organization of evidence documenting the organization's control assessment and remediation activities. This evidence provides management at all levels of the business with insight into the organization's risk and compliance status, and it makes the task of responding to auditors' requests simpler.

The focus of orchestration tools is to automate policy creation, policy review, risk assessment, controls assessment, remediation, and reporting activities. These tools help eliminate overlapping controls and improve the efficiency of risk management and compliance personnel.

Many enterprises find value in security compliance orchestration tools because they offer repeatability and scalability that's not easily achievable through manual means. Alternatively, they might acquire tools in response to regulatory mandates themselves, not just for process improvement. For example, the Federal Financial Institutions Examination Council (FFIEC) *Information Technology Examination Handbook* (http://www.ffiec.gov/ffiecinfobase/html_pages/it_01.html) has an "Information Security" section that states:

> Risk assessments for most industries focus only on the risk to the business entity. Financial institutions must also consider the risk to their customers' information. For example, the 501(b) guidelines require financial institutions to "protect against unauthorized access to or use of customer information that could result in substantial harm or inconvenience to any customer.

The document goes on to outline three aspects of a risk assessment process:

> Common elements of risk assessment approaches involve three phases: information gathering, analysis, and prioritizing responses. Vendor concerns add additional elements to the process.[1]

Many organizations look to a software product to help implement the information-security risk-assessment program. This is clearly one aspect of orchestrating compliance.

Compliance and Process

The fundamental activity of compliance is the generation of evidence. The compliance process involves assessing and generating evidence about the state of the business and the risks it faces, formulating and documenting policy to optimize the state of the business and balancing risks against rewards, and taking action (and generating evidence to document that action) to move the business toward the desired state.

One of the first questions related to security compliance orchestration is, "How can security teams relate compliance requirements to organizational policies and actual protective controls?" Burton Group's answer is to define and formalize technology and process requirements, manage them over time (through change-control efforts), and automate those things for which there are mature, cost-effective solutions.

The *Security and Risk Management Strategies* overview "A Systematic, Comprehensive Approach to Information Security" describes key steps of the process: business requirements must drive a risk-management process, which leads to creation of organizational security policy and a related control framework, which leads to technology architecture (e.g., guidelines and standards for control activities), the implementation of which results in technical policy management and feedback.

Compliance requirements and risk management must go hand-in-hand. Indeed, compliance is one of the critical elements of risk assessment, and risk-assessment tools discussed in this report can help security architects begin the process of automatically deriving requirements. Organizational security policy is determined by business drivers, compliance mapping, and risk assessment. Security-policy-management tools discussed in this report can provide assistance in automating the creation and dissemination of policies. Protective controls should flow from the policies and security architecture, and they must encompass both technical and nontechnical mechanisms. In order to assess controls, organizations need more than technical policy-management tools: they need automated self-assessment (i.e., surveys) that can test the effectiveness of processes that aren't technological. Security compliance orchestration tools provide such a capability.

Many Product Requirements

Risk assessment is not the only piece of the puzzle, though. What does a security team need in order to manage security compliance? Products can never provide the full solution, but they can offer several elements of automation that streamline the process and/or reduce errors. Furthermore, products can provide a knowledgebase of regulations and control standards that, while not exactly matching enterprise-specific requirements, can help security practitioners gain a head start in policy development and assessment.

Security compliance orchestration products have the following characteristics and capabilities:

- They offer a knowledgebase of regulations and control standards.
- They aid in creating and managing organizational security policy.
- They help import organizational security policy.
- They provide templates for default controls.
- They facilitate assessment of technical-infrastructure assessment.
- They offer assessments based on factors outside the technological realm.
- They enable security-compliance tracking.
- They offer feedback and reporting functions.
- They offer means of resolution.

Vendor solutions are described in "The Details" section of this report. Although other kinds of security products provide some of these features, they are often focused exclusively on technology management (rather than non-technology controls) and generally don't handle organizational policy. Vulnerability management, configuration management, entitlements review and attestation, security information and event management (SIEM), and large security suite tools are natural candidates for security compliance orchestration, but they fall short because compliance also requires non-technology oversight. This topic is covered at length in the "Market Impact" section of this report.

Knowledgebase of Regulations and Control Standards

In order to track organizational policies and compliance controls, a solution needs to meet fundamental requirements. Or, more accurately, a vendor must interpret regulations and define relationships to control objectives, security mechanisms, or manual controls. These requirements are generally found in regulatory mandates such as SOX, GLBA, or Health Insurance Portability and Accountability Act (HIPAA). They may also be found in control standards such as International Organization for Standardization (ISO) 17799/27001, National Institute of Standards and Technology (NIST) 800-26, Information Security Forum (ISF) methodologies, and IT Governance Institute's Control Objectives for Information and related Technology (CobiT). They can also be found in third-party obligations such as Payment Card Industry (PCI) security standards. For more information about these standards and frameworks, see the *Security and Risk Management Strategies* overviews "Enterprise Security Control Standards: Which Ones and Where They Apply" and "IT Risk Management and COSO."

A regulations and controls knowledgebase may be used as a template for the creation of policy and for assessment of an organization's technical or nontechnical controls.

Creation and Management of Organizational Security Policy

Organizational security policy is important. It sets expectations and the operational tone, and provides guidance for both technical-infrastructure choices and nontechnical controls. The lack of adequate policy documentation has reportedly caused findings of material weakness by some auditors. And, for a large organization, simply managing the lifecycle of bulky policies can be difficult. After a security score of "F"—due in part to inadequate policies—one U.S. federal agency created 1,700 pages of policy documents. Although that might have been overkill, managing such a tome would be nearly impossible without some automation.

Typical policy-management features include:

- The ability to collaborate during policy development
- Default templates from common policy elements
- Version control
- Workflows for policy approval
- The ability to digitally distribute policies to employees
- Employee-acknowledgment/acceptance capability
- Training/awareness functionality and the ability to test policy knowledge
- Reporting capabilities

Importation of Organizational Security Policy

In addition to creating policies from scratch, security compliance orchestration tools should also allow the import and management of existing policy text. They also should allow mapping between imported policies and relevant control standards, regulations, or underlying controls that an enterprise operates. Generally, such mappings must be done by hand, rather than automated. The positive aspect of mapping is that it can reveal holes in existing policies. The negative aspect is that a vendor tool might have a control framework that is considerably different than the organization's, in which case mapping will be difficult.

Templates for Default Controls

At the heart of compliance are controls that prevent negative outcomes, or, more accurately, reduce the risk of harmful occurrences. Although controls may be technological (e.g., a vulnerability scanner that monitors systems for security holes) many are non-technological; for instance, background checks for prospective employees or fire extinguishers in critical areas. Many technical-management solutions now add compliance links. For example, many configuration-management, vulnerability-management, and patch-management vendors have all added compliance-reporting features. However, because these solutions handle *only* technology controls, they miss a large part of the landscape.

One Burton Group client reports that more than 50% of its security controls are not technological, so a technical policy-management tool with a bit of SOX or HIPAA reporting would not be adequate. This sentiment is common among Burton Group clients, and it is echoed throughout this report: technical controls alone will not suffice for compliance. Therefore, technical policy management and assessment alone are insufficient.

The default controls in security compliance products have some key features. First, they represent both IT and non-IT mitigators. Second, the controls are mapped to high-level policies or compliance requirements, so security teams can detect gaps between requirements and operating controls. Third, the solutions provide means to assess whether controls are present and functioning. This may be through technical mechanisms (e.g., examining a host configuration setting), or through nontechnical means (e.g., surveying employees); most security compliance orchestration products include native technical mechanisms for automated data collection; many also integrate with third-party patch management, change management, and configuration management systems which serve as data feeds. And fourth, controls must be able to be mapped to all applicable regulatory requirements so that controls are not unnecessarily duplicated.

Completeness of coverage is also of paramount importance. A blended control set based on major control standards is probably the best approach—and it spares the security/compliance team from doing all the mappings themselves. Although all of the products have some form of codified control set, common areas should include:

- Business continuity
- Capacity planning
- Change control
- IT controls (including networks, servers, desktops, messaging, applications, Internet presence, and so on)
- Personnel controls
- Physical controls
- Training and awareness
- Vendor management (including outsourced services)

Technical-Infrastructure Assessment

Teams interact with three major classes of controls: First are IT controls implemented by technical solutions. Examples include anti-malware software, firewalls, and encryption. Second are IT controls that are less automated and that may be managed via procedures or other non-technological means. Examples include proximity-badge issuance and revocation, or locking a workstation when a user walks away. Third are non-technology controls such as physical locks and keys, clean-desk policies, rules for how to handle customer information over the telephone, fire-suppression devices, and so forth.

Fully automated technical controls can and should be assessed through software mechanisms. For example, if policies require patches to be deployed within three days, then a compliance-assessment tool should query patch-management solutions (and possibly individual hosts) to determine whether the policy is in effect. Often, products use agents of some sort to perform these queries. Polivec uses this approach. Other solutions assess technical inputs without the need for additional software. Symantec (through technology acquired from BindView) takes this approach. Many risk-assessment tools also allow for manual data input from technology systems.

Non-Technology Assessment

For infrastructure that cannot be queried via software or networks—and for non-technology controls—security compliance tools must provide a survey mechanism to determine whether controls are operating. One vendor's customers describe the solution as “TurboTax for compliance”—basically, for a particular control, the product asks questions that evaluate the effectiveness of the control, much like how tax-preparation software asks questions to assess tax status.

For example, if an organizational control objective is to ensure that systems are available for data processing, and the control is to reduce the harm from fire by placing fire extinguishers throughout the facility, then key employees may be asked, “How many fire extinguishers are available in your physical area?” Data-center personnel might be asked, “Does the server room have an automatic fire-suppression system?” By collating results from across the organization, the security team begins to understand whether fire controls are adequate.

In order to make this self-assessment survey process scalable, the solutions must provide support for authoring, distributing, completing, collecting, and documenting surveys. Solutions must automatically generate survey questions based on policies, compliance requirements, and controls selected by the organization. Surveys must be delegable to employees across the organization, based on their roles and areas of responsibility. The system must provide a workflow (generally one that is e-mail based) to send reminders to survey respondents. And the product must provide reporting on survey status, to allow tracking of self-assessment efforts.

Beyond mere surveys, an ideal state would be to embed assessment workflow into business and technology processes themselves. It is critical that at each important step—be it testing a fire extinguisher, performing personnel background checks, or verifying a vendor—a person follows a set of predetermined manual or automated criteria: they perform the task, make a determination, and complete their step in the process, while workflow and audit events are generated, passing the process on to the next person, and attesting that controls were effectively enforced. The workflow should also include an audit capability so that, for every security-related part of the process, there is management signoff, a testing or sampling event, or some other verification that is appropriate and cost effective. Security compliance orchestration vendors have made a lot of progress over the last two years in moving toward a robust embedded assessment workflow, by creating native workflow facilities, integrating with third-party ticketing tools, and automating features for design, distribution, completion, collection, and analysis of electronic surveys.

Security Compliance Tracking

Together, technical-infrastructure assessment and non-technology assessment provide a means to track compliance. The missing link is a map between low-level controls and compliance drivers. Many solutions provide a requirements traceability matrix to show how particular controls implement the requirements of governing regulation or policies.

Most products provide for a controls-gap assessment, in which the results of assessments are compared against a list of recommended controls for a particular high-level mandate. The product discovers which controls are missing or operating ineffectively. It is up to the security team to determine whether recommended controls can be ignored (perhaps by justifying on the basis of compensating controls or low business impact) and documented, or whether they should be remediated, possibly by adding additional controls or better enforcement of existing ones.

In general, tools are only as good as the basis of their assessment, which boils down to their codification of requirements traceability. Requirements should link to policies, which link to controls, which link to surveys. Otherwise, the assessment is of questionable value. Perhaps it's interesting to say, "We're 65% compliant with this arbitrary standard," but the real value is in assessing an organization's own policies (assuming they've been created in a systematic, comprehensive way). Even better are synergies between policy-creation tools and assessment tools, to improve the basis for all assessment. Although such convergence isn't complete, the emergence of blended tools shows this is an upcoming trend (which is discussed more in the "Market Impact" section of this report).

Feedback/Reporting

Clearly, solutions must provide a means to report results to various stakeholders, whether business owners, security teams, audit groups, or executives. This is accomplished through a variety of dashboards, graphs, and related reports. Security compliance orchestration tools increasingly provide role-based reports and dashboards, which customize status and remediation information to ensure that tool users receive only information relevant to their jobs and responsibilities.

Resolution

The final goal of orchestrating compliance is to find and plug holes. If infrastructure isn't behaving in accordance with policy, then technology should be reconfigured appropriately. If a nontechnical process is not providing adequate control, then it should be retooled. Many solutions can track action plans to resolve compliance problems and even launch workflows, but few of them reach out to change infrastructure. Burton Group believes that this is a wise choice; too much automation of infrastructure updates can easily be disruptive to operations, and it can also dilute accountability for changes and reduce personnel awareness of the state of the business and its systems. The right approach to remediating control gaps and other compliance and risk flaws is, in our view, to generate a trouble or incident ticket in a ticketing system (whether implemented as a native feature of the security compliance tool or provided through integration with a third-party ticketing system such as Remedy), and to implement and document the fix through the proper change control process or mechanism.

Security Compliance Orchestration Architecture

Figure 1 shows an architectural view of security compliance orchestration. It specifically shows these elements vis-à-vis the policy-management and risk-assessment tools discussed in this report.

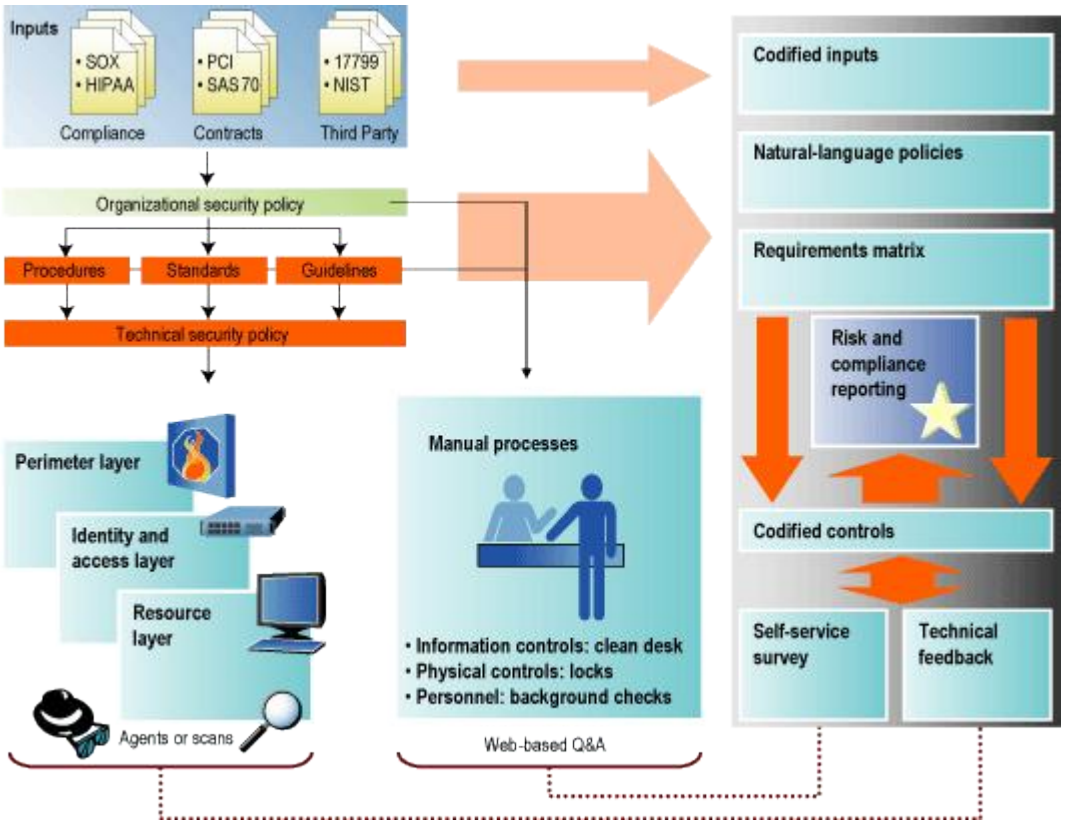

Figure 1: *Elements of Security Compliance Orchestration*

Security compliance orchestration products are increasingly providing all the elements of this solution, albeit each vendor's offering supports different functions at different levels of maturity and automation

Ideally, high-level compliance and contractual requirements would feed into organizational policies, which drive down to technical security policies (implemented by infrastructure components) and manual procedures to meet confidentiality, integrity, availability, use-control, and accountability obligations. At the same time, such inputs would map into compliance-orchestration solutions, which monitor both the technical and nontechnical controls to assess whether requirements are adequately satisfied.

Finally, two additional elements are required for security compliance orchestration. First is workflow, as mentioned previously. This is subsumed by the "self-service survey" and "risk and compliance reporting" boxes in Figure 1, but in current security compliance orchestration solutions workflow is emerging as a core feature that is tightly coupled to most, if not all, compliance-related processes. The second element is change control over compliance state (as opposed to change control over a particular policy), which is not part of the solutions described in this report, but needs to be a component of organizational compliance efforts. More information about change control can be found in the *Security and Risk Management Strategies* overview "Change Management for the Enterprise" and the Reference Architecture technical position "Change Management with Assurance."

Monitoring and Feedback

The types of controls that an organization can deploy and the means by which they can be assessed were described in the "Templates for Default Controls" section of this report. In essence, certain technology controls can be monitored via technical mechanisms like scans or software agents, whereas nontechnology controls must be assessed manually—typically through a user survey. However, there are some subtleties that should be discussed. Figure 2 provides some examples.

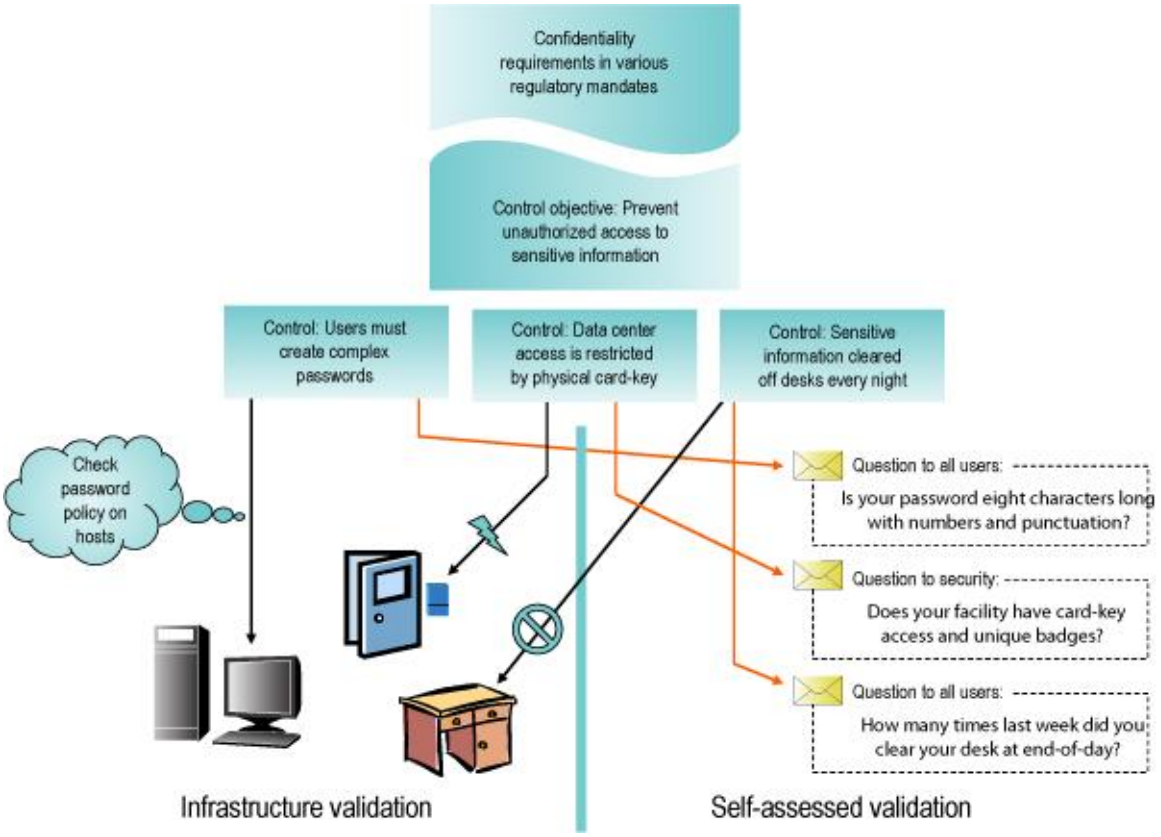

Figure 2: *Types of Compliance Analysis: Infrastructure Monitoring (Technical Feedback) and Self-Assessment (Surveys)*

Consider an organization whose objective is to protect confidentiality, so it has instituted controls to protect computer use, to prevent unauthorized access to premises, and to ensure paper information is not left out for prying eyes. Each of these controls needs to be assessed to determine whether policies and compliance obligations are met. How can the organization achieve this? Table 1 provides a synopsis.

Control	Validation through infrastructure	Validation through survey
Password policy	Password policies are often administered through a technical policy-management solution. Even if they are not, individual hosts can be queried for password settings. Therefore, this control can be safely assessed through the infrastructure.	A self-service survey could ask users about characteristics of their passwords, which would yield an appropriate assessment. However, users could answer questions incorrectly, so infrastructure validation is a better approach.
Data center physical access	A card-key system often has a management console that runs reports on access. Such information could be fed into a compliance tool to ostensibly test access controls. However, this approach is incomplete. Although it measures the presence of the control (e.g., "Is there a card reader in the New York data center?"), it does not measure effectiveness—such as whether tailgating occurs or badges are shared.	Physical-access control is often better assessed through a survey, or at least complemented with a survey, in order to discover whether users behave in accordance with policies, and that appropriate infrastructure is deployed for enforcement.
Clean desk	An entirely nontechnical control (e.g., a clean-desk policy) cannot be assessed using an infrastructure mechanism.	A survey is the only way to assess this control. However, there are unique ways to tackle the assessment. For example, in addition to asking users about their behavior, a survey could also query late-night cleaning crews to see if their observations about clean desks corroborate.

Table 1: *Validation of Different Controls*

There are other—and, in some cases, better—ways to validate controls. For example, to assess physical-access control, security teams could periodically review video logs, and auditors could verify with spot checks. Both of these activities could be coordinated by automated workflow to ensure that they happen regularly. Another option (which should probably be used only in high-risk situations, as it is very expensive) is to spot-check by physical-penetration test, with attestation of results through workflow and validation checks of the attestations by audit groups. In a related vein, workflow could require managers to periodically attest to the clean-desk conformance of their employees, with auditors validating the assertions.

Mapping controls and infrastructure to higher-level policies or regulatory requirements is one of the challenges of security compliance orchestration. Products take different approaches to the problem. Risk-assessment solutions generally use assessment questions as the core linkage. Policy-oriented tools generally provide some mapping function between policy statements and controls. For example, Symantec uses a novel canvas tool that eases the process of mapping among different layers of the compliance stack. However, it's important to remember that such a tool cannot replace the need for human intelligence in determining valid measurements and assessments.

Market Impact

It's important to understand the context within which security compliance orchestration tools have emerged. Tools have moved into security compliance orchestration from three directions: security-focused tools have moved into security compliance orchestration from the risk assessment market; compliance-focused tools have moved into security compliance orchestration from the audit and compliance automation market, and orchestration-focused tools have moved into security compliance orchestration from the system management and policy management market. Figure 3 places today's security compliance orchestration vendors on this map, and illustrates how the compelling security compliance orchestration value proposition (i.e., reduced cost of controls and reduced cost of compliance) is leading each vendor in the space to move into the "security compliance orchestration gravity well" at the center of the diagram by developing a complete spectrum of features. McAfee doesn't appear on Figure 3's Venn diagram, but readers should think of McAfee as "coming in from all directions" on the diagram, because McAfee has assembled a portfolio of assets (notably McAfee ePolicy Orchestrator, McAfee Risk and Compliance Manager, and McAfee Vulnerability Manager) that approach security compliance orchestration from all directions.

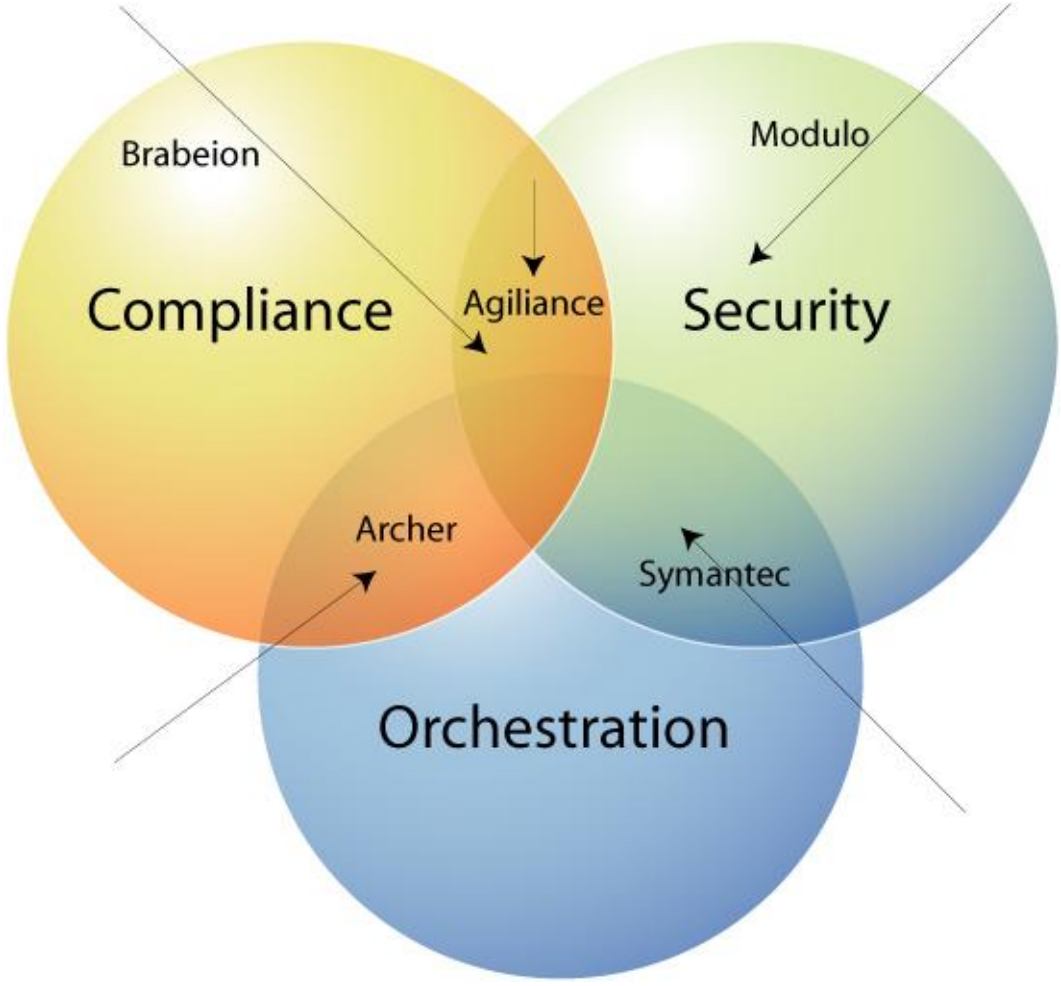

Figure 3: *Development of the Security Compliance Orchestration Market*

The primary business drivers for the security compliance orchestration market are well aligned with the core governance, risk management, and compliance goals (i.e., building value and creating organizational transparency) enumerated in the *Security and Risk Management Strategies* overview "Governance, Risk, and Compliance"; the top business drivers are:

- Value creation through elimination of redundant controls responsive to multiple regulations

- Risk reduction through reduced dependence on manual spreadsheet-based compliance and control activities
- Improved audit performance through improved documentation of compliance status, improved time-to-fix, and more persuasive documentation of risk basis of controls and remediation of deficiencies
- Improved organizational transparency through consistent, organization-wide, reliable reporting of risks and status of controls

Closely allied tools are growing up around this developing market, as illustrated in Figure 4. Closer to the executive suite, where the chief executive officer (CEO) and the board sit, are the enterprise and financial governance, risk management, and compliance tools offered by vendors like OpenPages and Paisley.

Farther from the executive suite, on the main floors of the building where the system administrators and first-line managers work, are a set of specialist tools which gather very detailed information about specific risk- and compliance-associated phenomena, including user roles and entitlements (SailPoint, Aveksa, Sun Microsystems/Vaau, Oracle/Bridgestream), data classification and business need-to-know (Varonis), and financial and management roles, compliance obligations, and resource access authorizations (Approva).

And in the basement, on the raised floor of the machine room, where the chief information officer (CIO)'s staff and the chief information security officer (CISO)'s staff do their jobs, are the security compliance orchestration tools detailed in this report.

It would not be at all surprising to find a single organization which deployed OpenPages, Approva, Archer Technologies, SailPoint, and Varonis (or another equivalent combination of vendors occupying different floors of the building). Indeed, several vendors on different floors have formal or informal partnerships, and other pairs of vendors are currently investigating partnership. This coexistence is an excellent illustration of why “IT-GRC” is useless as a description of a market; it applies to many vendors whose offerings are complementary rather than competitive. Indeed, even in the core security compliance orchestration space there are still synergies. At least one customer Burton Group interviewed uses tools from both Brabeion Software and Archer.

Furthermore, every vendor interviewed for this report lists “Excel spreadsheets” as their primary competitor. Clearly, organizations considering implementation of security compliance orchestration should take care to specify the actual functions they are seeking to automate, and should not choose vendor shortlists from some notional list of “IT-GRC” vendors.

Market Segmentation

Figure 4 shows an at-a-glance view of various solutions that might play a role in security compliance orchestration. This report focuses primarily on security compliance orchestration tools, but these tools coexist—and, in some cases, integrate—with tools on the higher floors of the building.

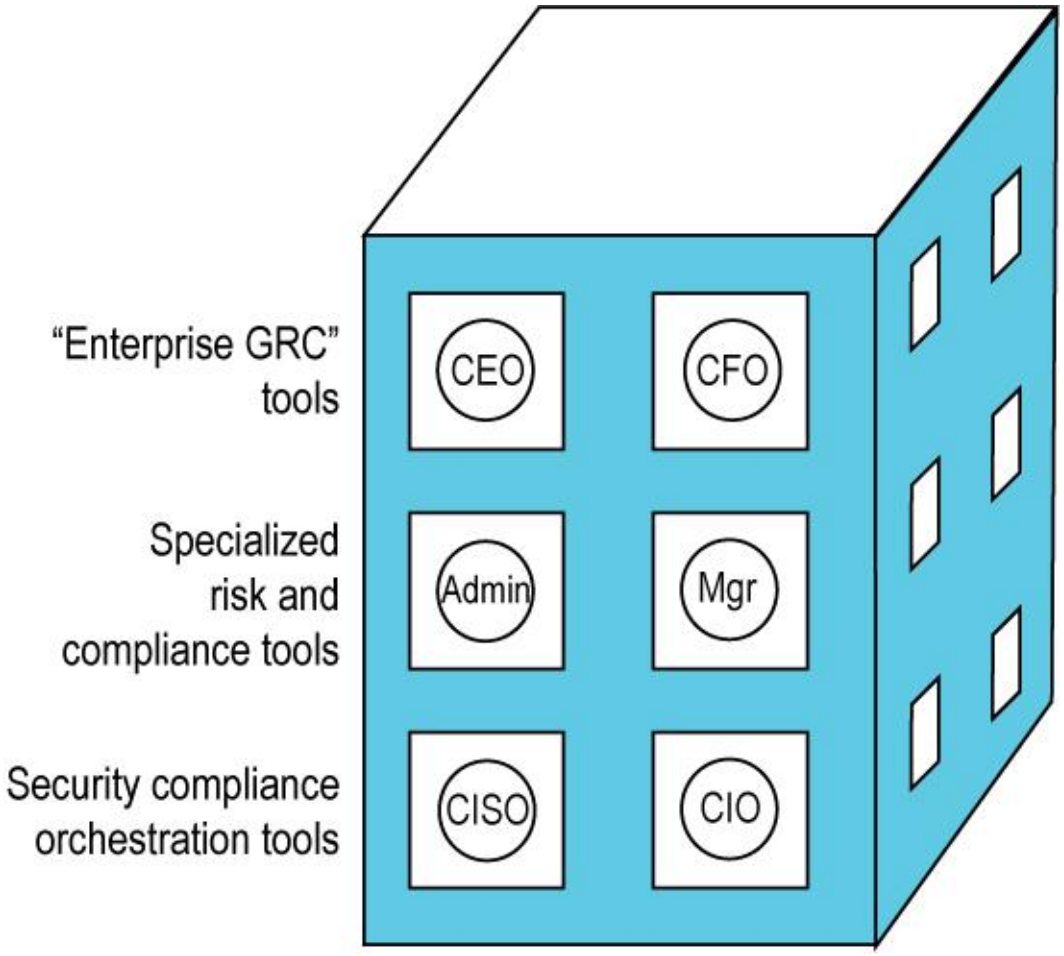

Figure 4:*Tools for Various Aspects of Security Compliance, Policy Management, Compliance Management, and Risk Assessment*

Customer Segmentation

Market segmentation is often analyzed by customer types, as well as vendor types, but in this case it's fairly straightforward. There's little reason to orchestrate compliance unless an organization has something to comply with. Therefore, regulated industries are the most likely targets for all types of compliance-orchestration tools. Government agencies also tend to be major customers of risk-assessment products, although expansion into the commercial sector is commensurate with increased commercial-sector regulatory scrutiny. Large corporations tend to be the targets for policy-management and blended tools (including security suites). But emerging service-provider offerings will allow vendors to move down market.

Market Dynamics

The real competition for security compliance automation tools is the Excel spreadsheet and the corporate IT department. All security compliance orchestration vendors report that they tend to displace software and spreadsheets that their customers build in-house. One Burton Group client points out that it sends 1,000 surveys monthly using existing desktop-management tools but patches together an amalgam of products to assess and report results.

But the days of compliance management by Excel are numbered—and the number is small. Auditors and corporate executives are demanding more reliable, credible, and comprehensible reports. These reports cannot be generated in an ad-hoc fashion using primitive tools. The scope and complexity of the systems and processes to be assessed is simply too great. And frankly, it's to an organization's benefit to automate such tasks: Not only will assessment become repeatable and hence less error-prone, it will bring cost efficiencies and a lighter audit burden (because auditor requirements for sampling tend to drop when control processes are automated).

The security compliance orchestration market has formed around this demand, and all of the vendors are falling into the black hole at the center of Figure 3's Venn diagram. Today's vendors are still differentiated by security/compliance/orchestration orientation and by relative maturity of different parts of the core security compliance orchestration feature set. But this will not last; these vendors will be forced by corporate executives, CIOs, auditors, and regulators to become more and more like one another. McAfee is a leading indicator of this trend, with its increasingly integrated portfolio of security, compliance, and orchestration assets, some developed in-house and some resulting from acquisitions.

As further consolidation and integration happens over the next two years, competition will heat up between these vendors, and some consolidation of the security compliance orchestration market may occur as platform players like IBM, Oracle, Sun, and CA fill the currently substantial compliance orchestration holes in their portfolios.

At the end of this first phase of consolidation, customers should expect to see one or two leading independent security compliance orchestration vendors and a number of platform players (including Symantec, which already has an offering) with integrated security compliance orchestration offerings.

A second phase of consolidation is likely to begin at that point. The demands of governance, which Burton Group defines (in the *Security and Risk Management Strategies* overview "Governance, Risk, and Compliance") as roundtrip management, will exert pressure to integrate security compliance orchestration vertically—that is, to integrate offerings from the different floors of the building in Figure 4. Increasing demands by senior executive managers for drill-down insight into the details underneath their enterprise and financial governance, risk management, and compliance dashboards will exert pressure for integration of enterprise and financial "GRC" products like OpenPages and Paisley with security compliance orchestration offerings. And pressure to expand visibility beyond system configurations and vulnerabilities into business roles, entitlements, application configurations, and business processes will drive integration of security compliance orchestration products with non-security (i.e., financial, identity, application) orchestration offerings like those currently provided by Approva, Aveksa, SailPoint, Varonis, and others.

The end result won't be ready for deployment and use for five years. But when "it" is ready for deployment, what "it" may be (if we're lucky) is a true governance tool: a roundtrip management platform which makes the organization's technical and process operations transparent to management at all levels and allows effective assessment and management of IT and business risk.

This roundtrip management platform won't be the all-singing, all-dancing, one-stop-shop, lights-out tool that takes humans out of the governance, risk management, and compliance loop. That tool doesn't exist, won't exist, and can't exist. Governance, risk management, and compliance are all fundamentally dependent on human judgment. But human judgment can be improved by better information, and human drudgery can be relieved by good tools. A strong compliance orchestration platform—encompassing not only security compliance orchestration but other aspects of compliance and risk management too—can and will make organizations more effective at all three activities. Even when the platform is in place, Burton Group believes there will still be a need for specialist tools—especially in the area of risk management—to complement the platform capabilities.

Recommendations

First, organizations should carefully ignore “IT-GRC” hype and confusion. The “IT-GRC” label is applied fairly indiscriminately to a wide variety of tools with very different and often complementary functions. Organizations should carefully study what compliance, risk management, and governance problems they want to solve, and then evaluate tools on the basis of their ability to address those problems. Since even the market for security compliance orchestration solutions is still somewhat immature, it's important not to make the short list too short. It may be that a combination of tools—even tools which at the level of the marketing brochure seem to compete—may be much more effective than a single tool when applied to an organization's actual problem.

Organizations should pay special attention to policies and nontechnical controls. These are too often overlooked by technology-minded security practitioners, and the result can be painful audit findings—or actual losses due to incidents. In order to scale the process of manual controls assessment, carefully evaluate workflow and survey functionality of the tools being considered. It should be noted that out-of-box questions will probably not fully cover the controls requirements for most organizations. Expect to refine the assessment process and customize it for individual business processes and unique control choices.

Enterprises should focus on tools that match their organizational style. One of Burton Group's insurance-industry clients reported that too much quantitative analysis paralyzes its team. The client requires a much more qualitative treatment of risk—such as high/medium/low, rather than percentage likelihood of a particular threat or probable annual dollar loss (which it can't rationalize to management). So a numbers-heavy tool like Agiliance may not work for this client. Although the assessment model approved by NIST is compelling, sometimes it's too much effort to evaluate the probability of various disaster scenarios and what the rebuilding costs would be.

Many organizations are looking for gap analyses of controls and policies rather than numeric risk ratings. Any given product's basis for risk measurement may not align with organizational needs (see the *Security and Risk Management Strategies* overview “Security Metrics: Horses for Courses”), and management is unlikely to respond favorably to arbitrary numbers, whereas demonstrably inadequate controls are persuasive from an audit perspective. In addition, some organizations want hard numbers, costs, and dollars that have been evaluated mathematically. In such cases, a tool which supports return on investment (ROI) analysis of controls (such as Agiliance or Modulo Risk Manager) fits the bill.

Enterprises should create requests for proposals (RFPs) with clearly defined and detailed requirements. Some client RFPs lack the proper level of detail. For example, one Burton Group client wanted a risk-assessment tool that “had a knowledgebase of the major best-practices standards (such as ISO 17799, CobiT, COSO, and NIST).” It turns out the “such as” phrase is very important. The security team should select and implement a control standard *first*, and thereafter it should deploy a compliance-orchestration solution to monitor its effectiveness. Therefore, when choosing a policy-management, risk-assessment, or blended tool, the *actual* control standards and regulatory mandates should be established before a security compliance orchestration vendor selection process is initiated. An organization should select a product that has a strong knowledgebase of the enterprise's specific choices. That's not to say that some additional customization won't be required, but be clear what guiding standards and requirements are critical.

The origination of the knowledgebase is important, too. Although Archer Technologies has created an impressive technology platform and cross-functional modules, its content libraries follow a type of community development model, which doesn't assure the same level of quality as those provided by firms with specialist regulatory and controls experience such as Brabeion, Agiliance, and Modulo. On the other hand, Archer's customer portal can be a helpful means of assessing trends and connecting with other organizations that suffer under difficult compliance requirements. Be mindful that, for most vendors, “the squeakiest wheel gets the knowledgebase” (in lieu of grease, one supposes). In other words, what gets developed is based on who cries loudest.

The exception may be proprietary module development, in which case the enterprise has to balance between personnel and product investments. Archer relates that one of its financial-services customers has developed more than 80 customized modules. The implication is that the solution has powerful technology underpinnings but may require considerable customization to link various components (e.g., risk management, threat management, and asset management). Enterprises must decide how much custom development they are willing to take on.

Although this report doesn't propose a formal maturity model for compliance orchestration, it is implied when talking to clients. Some teams still have essential controls to deploy and are not ready for an overarching policy-management or risk-assessment tool. For example, the security team from one of Burton Group's manufacturing client was evaluating a huge list of prospective compliance tools, and when they spoke to the operations team they discovered that the biggest pain point was configuration management and change control. When the security team examined possible reports and controls of such technical policy-management tools, they found them to be adequate for present needs. There's little doubt that they'll want higher-order compliance tracking in the years to come, but for now a more operational tool is most appropriate.

Finally, because the market is not yet fully mature, it's important to consider the orientations of the various security compliance orchestration vendors, and decide which vendor's orientation best suits a particular customer's compliance orchestration needs.

Organizations whose internal IT shops are politically powerful and might resist a packaged solution may find Archer's customizable framework, solution white-labeling option, and community exchange (whereby modules and design ideas can be exchanged with other customer organizations) very attractive.

Organizations that have immature risk management practices and need extensive guidance from a control framework will be attracted by Brabeion's mature knowledgebase, with its extremely detailed instructions for assessing controls and remediating weaknesses, and by its ability to both test controls directly against organizational policies and report detailed results.

Organizations with very strong risk management disciplines, on the other hand, will certainly be attracted by Agiliance's advanced risk metrics and sophisticated risk analysis and remediation workflow capabilities.

Organizations with extensive exposure to non-IT or non-information-security regulations will find Modulo Risk Manager's advanced survey support and strong organizational and geographic risk assessment capabilities very attractive.

Organizations that need to integrate risk management with incident management will find Symantec's bundling of security compliance orchestration and security event management (SEM) functionality compelling.

Organizations looking for an integrated portfolio of risk, threat, vulnerability, and policy management products will find the breadth of McAfee's offering set attractive.

The Details

Many vendors provide a small to medium-size slice of security compliance orchestration. To narrow the field for this report, some basic criteria had to be met by potential solutions:

- The report focuses only on products, not on service offerings.
- The solution must have an understanding of overarching compliance standards and/or requirements (e.g., Sarbanes-Oxley Act [SOX], International Organization for Standardization [ISO] 17799).
- The solution must help orchestrate compliance. That is, it must provide feedback to decision makers in some way to improve the state of security-related compliance.
- The solution must integrate treatment of automated and manual (survey-based) assessments.

Within these broad criteria, a product had to support the following specific functions to be considered a Security Compliance Orchestration offering:

- System configuration assessment
- Policy assessment
- Policy creation
  - Authoring support
  - Policy planning (e.g., templates)
  - Policy authorization workflow support
- Attestation
  - Periodic review of entitlements granted
- Compliance reporting
  - SOX compliance report generation
  - PCI DSS compliance report generation
  - GLBA compliance report generation
- Risk assessment
  - Identification of hazards
  - Estimation of hazard probabilities
  - Estimation of hazard consequences
- Vulnerability assessment (can be provided by integration with another tool)
  - Identification of systems' technical weaknesses
  - Identification of process deficiencies
- Control effectiveness auditing
  - COSO report generation
  - ITIL report generation
  - ISO 17799/27001/27002 report generation
  - CobiT controls report generation
- Control coverage auditing
  - Gap assessment
  - Remediation tracking
- Non-technical controls self-assessment
  - Survey design
  - Survey distribution
  - Survey results aggregation and reporting
- Exception logging and remediation tracking

The vendors who meet these criteria are: Agiliance, Archer Technologies, Brabeion Software, Modulo, and Symantec. McAfee and NetIQ offer similar solutions which are not covered in detail in this report. McAfee's product portfolio is profiled in the*Security and Risk Management Strategies* Product Profile document "McAfee Vulnerability Management Products."

Agiliance

Founded in 2005, Agiliance (www.agiliance.com) has built its product from the ground up as an integrated risk management and compliance solution. Agiliance IT-GRC 3.0 was released in November 2007, and is targeted at the needs of heavily regulated companies in all market sectors that face the need to comply with multiple regulations and want to take a risk-based approach to compliance. E-commerce providers to whom IT is a critical strategic asset, and at large enterprises whose IT organizations have recognized the need for a dedicated risk management function, are examples of customers in this target market.

Agiliance's key differentiators are:

- It is a solution which has been built from day one as a software product rather than as an adjunct to a consulting practice.
- It has a focus on moving organizations from a manual or semi-manual controls inventory and testing process to automated collection of risk and control information via electronic surveys and via agentless connectors to security and change-management systems. Agiliance believes that automated collection of information increases auditors' and other parties' confidence in the accuracy and completeness of the information. Agiliance recently acquired Phulaxis to augment the set of connectors which allow Agiliance to monitor and control databases, identity management (IdM) systems, and enterprise resource planning (ERP) systems.
- It has a rich set of advanced risk metrics.

Agiliance IT-GRC provides an asset information repository, in which it stores risk and compliance status information for a wide variety of IT assets. This information is gathered in an agentless fashion by connectors; information sources include vulnerability scanners, configuration management databases (CMDBs), security information management/security event management (SIM/SEM) products, IdM products, databases, and ERP systems, among others. Information can also be gathered in a manual or semi-automated fashion using electronic surveys, whose construction and distribution the product facilitates.

Agiliance IT-GRC incorporates a set of Common Control Framework libraries, against which asset information is compared to generate risk scores and exception reports. Control frameworks represented in this set of libraries include Control Objectives for Information and related Technology (CobiT), ISO, Information Technology Infrastructure Library (ITIL), National Institute of Standards and Technology (NIST), and Federal Financial Institutions Examination Council (FFIEC). The Common Control Framework libraries also include information about the control requirements of regulations including SOX, Payment Card Industry (PCI-DSS), Health Insurance Portability and Accountability Act (HIPAA), Gramm-Leach-Bliley Act (GLBA), Federal Information Security Management Act (FISMA), and North American Electric Reliability Corporation-Critical Infrastructure Protection (NERC-CIP).

Finally, Agiliance incorporates a variety of advanced risk assessment and scoring algorithms, including the ability to calculate separate risk scores for confidentiality, integrity, and availability; calculation of annualized loss expectancy (ALE) for individual assets; ability to calculate and track key risk indicators (KRIs) using metrics established by the Risk Management Association.

Agiliance IT-GRC 3.0 is licensed on a per-monitored-asset basis (where assets are servers, operating systems, applications, business processes, or other artifacts for which customers identify a monitoring need). An average deployment costs about $175,000.

Table 2 summarizes Agiliance IT-GRC 3.0's features.

Orchestration element	**Product capabilities**

Knowledgebase of regulations and control standards	Out-of-the-box Common Control Framework libraries incorporate information about control frameworks (including CobiT, ISO, ITIL, NIST, and FFIEC) and regulations (including SOX, PCI, HIPAA, GLBA, FISMA, and NERC-CIP).
Creation of organizational security policy	IT-GRC 3.0 assesses current protection posture versus chosen control framework or frameworks and then prioritizes departures from recommended controls via assessment of business risk.
Importation of organizational security policy	Common Control Framework contains control recommendations from a wide variety of standard control sets.
Default controls	Common Control Framework provides default control baselines and customizes policy using an included library of over 10,000 discrete controls. Assets to which risk assessments and controls can be applied include not only IT assets (e.g., servers, routers, applications, and operating systems) but also non-IT assets including people, vendors, and partners.
Technical-infrastructure assessment	IT-GRC 3.0 provides automated agentless testing of controls via integration with a variety of tools, including vulnerability scanners, CMDBs, SEM products, ERP systems, and other security automation offerings.
Non-technology assessment	IT-GRC 3.0 collects risk and compliance information via direct human attestation through the product's interface and via e-surveys.
Security compliance tracking	Survey results are analyzed by comparison with control framework recommendations; departures from recommended controls are assessed using risk-scoring algorithms and are prioritized according to risk. Results are aggregated and reported on customizable, role-based risk dashboards.
Feedback/reporting	Visual risk dashboards can be customized to the role of the viewer (e.g., auditor, chief financial officer [CFO], and internal auditor). Decision tools—including mitigation return on investment (ROI) analyzer, ALE view, and trend analysis—can be used to assist in mitigation decisions.
Resolution	Risk-prioritized remediation reports can be acted upon using a native ticketing system or via two-way integration with an external ticketing system such as Remedy. Product suggests mitigation actions.

Table 2: *Agiliance IT-GRC 3.0 Features*

Archer Technologies

Founded in 2000, Archer Technologies (www.archer-tech.com) has principals with roots fairly deep in the enterprise risk and compliance realm. As part of its sales strategy, Archer Technologies brings services and software customization to its customers, which are Fortune 1000 companies, primarily through direct sales but also through a portfolio of partnerships. Archer Technologies serves many verticals, but it has been particularly successful in financial services, pharmaceuticals, telecommunications, technology, and media; recently, it has been expanding its market into the retail sector. Although Archer Technologies provides training and limited services on its technology, the company is squarely a software provider and not a consultancy; in fact, Archer partners with consultancies and audit firms in compliance and risk management contexts. Archer provides direct, on-premises deployment; it also supports Software-as-a-Service deployment and a hosted-service offering for organizations that do not wish to deploy the product locally; IBM Global Services hosts Archer for its customers.

Archer Technologies' key differentiator is a technology platform that provides underlayment for a number of higher-level software applications. Called the Archer Technologies SmartSuite Framework (currently version 4.1.3, though an upgrade is in the works for Q2 2008), the technology provides fundamental services such as knowledgebase, user-portal and access control, workflow and alerting, management reports and visualization, field and application configuration, and so on. These capabilities can be combined into applications that satisfy a particular business need (e.g., asset management, policy development, or vendor-relationship management). The Archer SmartSuite Framework is essentially a toolkit which allows customers to automate their existing (or planned) compliance and risk management disciplines—though Archer provides some compliance and risk-management applications out of the box, and others are made available by Archer customers to other customers through the Archer Exchange online community. Archer encourages its customers to white-label Archer deployments with the customer's own branding, and the company believes that this white-label branding helps its customers avoid employee resistance to the use of the tools.

Most specific to security compliance orchestration is Archer Technologies' Enterprise Risk and Compliance solution suite, which includes the following applications:

- **Policy Management:** Creates and manages organizational security policies with mappings to guiding control frameworks
- **Risk Management:** Assesses technical and nontechnical controls based on policies developed in the Policy Management application
- **Threat Management:** Receives network intelligence feeds from third-party vendors and provides some correlation with the Asset Management application's knowledge of IT resources
- **Asset Management:** Imports data—such as business process, business unit, applications, technology assets, and facilities information—from existing asset repositories to monitor risk/compliance status of both IT and non-IT resources in the organization
- **Incident Management:** Provides workflow and case management for various incidents—including security breaches, fraud, physical events, and accounting problems—across an organization. Incident management is integrated with helpdesk systems (e.g., Peregrine Systems and Manage Now) for trouble ticketing
- **Vendor Management:** Manages controls, processes, and interactions with vendors to ensure consistency and compliance with security requirements, as well as to increase the efficiency of business interactions
- **SOX Compliance Management:** Automates and manages SOX governance initiatives, assesses compliance deficiencies by business unit, and tracks remediation processes related to operational risk

Archer Technologies does not provide a direct enforcement capability. Rather, it works with technical policy management vendors (e.g., Altiris/Pedestal Software or Symantec/BindView) to remediate infrastructure issues.

Archer's product is priced based on an enterprise license, and an average license costs about $186,000 annually.

Table 3 summarizes Archer Technologies' solution-suite features.

Orchestration element	**Product capabilities**
Knowledgebase of regulations and control standards	Several applications use Archer Technologies' underlying knowledgebase functions to encode and map regulations and control standards. Most notably, the Policy Management and Risk Management applications have codified prominent controls related to SOX, CobiT, ISO 17799, HIPAA, Information Security Forum (ISF), and others. However, knowledgebase creation is accomplished through a "community development" model, meaning that controls may have been composed by another customer rather than Archer Technologies itself.
Creation of organizational security policy	Organizational security policy can be created from scratch or composed using provided templates.

Importation of organizational security policy	Existing natural-language policies can be imported into the Policy Management application, and users can specify a mapping of controls to regulatory drivers for subsequent assessment activities as part of the import configuration.
Default controls	Both IT and non-IT controls are included in the Policy Management application. The range of controls is quite broad—from router-configuration standards that discuss implementation of Internet Control Message Protocol (ICMP) handling to physical controls around public meeting spaces.
Technical-infrastructure assessment	Threat Management and Asset Management information can be tapped to analyze IT-related issues, especially regarding system vulnerabilities and other potential security problems. For tighter link to the Risk Management application, some customers use the Archer Technologies application programming interface (API) to link technical policy-management solutions (e.g., query a system-management tool for a certain host setting, and automatically fill out the Archer Technologies risk-assessment survey based on answers).
Non-technology assessment	Archer Technologies' Risk Management application provides a self-assessment survey mechanism. Risk scoring can be configured by the organization, or it can be automated, based on asset criticality and other factors. Delegation of the survey can be automated through creation of user and group fields which drive automated routing of assessment surveys.
Security compliance tracking	Survey results can be linked to control standards or regulations to reveal compliance per question or assessment area.
Feedback/reporting	Management reporting and visual dashboards are a fundamental component of the Archer Technologies framework. Alerting and workflow capabilities also allow near-real-time notification of issues.
Resolution	Archer Technologies' applications do not directly resolve problems; they tie to third-party technical tools to fix issues. Case-management capabilities in the Incident Management application can help accommodate higher-level problem tracking and resolution.

Table 3: *Archer Technologies' Enterprise Security Management Solution Suite Features*

Brabeion Software

Founded in 2004, Brabeion Software (www.brabeion.com) has leveraged PricewaterhouseCoopers (PwC)'s extensive compliance and risk management knowledgebase to create a packaged security compliance orchestration product called the Brabeion Polaris Suite. The suite includes three elements: The Polaris Knowledgebase, Polaris Pathfinder 7.1, and Polaris Navigator 3.1. The Knowledgebase includes PwC's database of IT standards, control framework requirements and individual technical configuration controls, and implementation steps required to implement controls on various platforms which Brabeion has mapped to regulatory requirements and control frameworks. The Knowledgebase also includes Brabeion-built policies and survey questions supporting a variety of regulations plus ITIL. Polaris Pathfinder 7.1 is a workflow automation tool which includes content lifecycle management; communication of policy, standards, and control information; and communication of implementation procedures derived from the Polaris Knowledgebase). Polaris Navigator 3.1 is a business-role-based compliance and risk assessment query and reporting dashboard designed to enable a closed-loop risk identification, compliance gap assessment, remediation, and evidence collection process that is supported by both automated collection of information about general computing controls and manual assessments of people, processes, and technologies. The suite's current user base consists entirely of Fortune 350 companies. Its pricing model incorporates charges per server, per monitored system, and per user seat. Enterprise licensing is available; an average deployment costs about $250,000.

Brabeion's key differentiators are:

- It has an extensive control, compliance, and risk assessment knowledgebase incorporating licensed technology configuration control content from PwC, supported by collaborative workflow tools to manage the lifecycle of policies, standards, and controls.
- It has a robust and extremely detailed mapping of control framework requirements to specific controls and the steps needed to implement those controls on individual target systems.
- It has a workflow which generates detailed evidence of regulatory obligations, control requirements based on these obligations, control deficiencies in deployed systems (measured against actual policies and control configurations adopted by policy), required remediation actions and responsibility for those actions, and actions actually taken in response to the remediation requirements.
- It offers support for exception management (this allows remediation of gaps to be deferred based on low assessed risk or other factors, and generates evidence of the rationale for deferral).

Brabeion holds an exclusive license from PwC for the technical control configuration contents of the Polaris Knowledgebase. The knowledgebase contains detailed information which Brabeion has mapped to more than 30 regulations and control frameworks including CobiT, The Committee of Sponsoring Organizations of the Treadway Commission (COSO), ITIL, NIST, ISO, SOX, GLBA, HIPAA, FFIEC, PCI, and NERC.

The knowledgebase also contains information about steps needed to implement more than 6,000 individual controls on more than 90 individual target technologies including all major operating systems and databases, many networking components, and a wide variety of other offerings.

The Polaris Suite offers risk assessment through automated collection of information about gaps in control coverage versus applicable regulations and through distribution and collection of manual surveys.

Table 4 summarizes the Brabeion Polaris Suite's features.

Orchestration element	**Product capabilities**
Knowledgebase of regulations and control standards	Polaris knowledgebase, licensed from PwC, includes information about requirements of over 30 regulations and control frameworks, including CobiT, COSO, ITIL, NIST, ISO, SOX, GLBA, HIPAA, FFIEC, PCI, and NERC.
Creation of organizational security policy	Polaris Suite assesses current protection posture vs. chosen control framework or frameworks; it customizes policy based on applicable regulations and unique business requirements. Workflow enables collaborative policy authoring and review.

Importation of organizational security policy	Polaris Knowledgebase contains control recommendations from a wide variety of standard control sets.
Default controls	Polaris Knowledgebase contains baseline control recommendations for a wide variety of regulations and control frameworks; it also customizes policy using included library of over 6,000 discrete controls. Specific controls are included for more than 90 target IT system types.
Technical-infrastructure assessment	Polaris Suite offers automated agentless testing of controls via integration with a variety of tools, including vulnerability scanners, SEM products, and configuration-management and change-management systems.
Non-technology assessment	Polaris Suite collects risk and compliance information via direct human attestation through the product's interface and via e-Surveys.
Security compliance tracking	Survey results are analyzed by comparison with control framework recommendations; departures from recommended controls are assessed using risk-scoring algorithms and are prioritized according to risk. Results are aggregated and reported on customizable, role-based risk dashboards.
Feedback/reporting	Visual risk dashboards can be customized to the role of the viewer (e.g., auditor, CFO, and internal auditor). Risk impact is assessed based on criticality, value, confidentiality, integrity, and availability. Automated assessments and survey results can be consolidated on a single dashboard.
Resolution	Detailed remediation reports derived from system configuration information in the Polaris Knowledgebase can be acted upon using a native, role-based workflow.

Table 4: *Brabeion Polaris Suite Features*

McAfee

McAfee approaches security compliance orchestration with a portfolio of products, incorporating both in-house technology and assets resulting from its acquisitions of Preventsys and Foundstone. The McAfee compliance and risk management portfolio includes McAfee Risk and Compliance Manager (formerly McAfee Preventsys), McAfee Vulnerability Manager (formerly Foundstone Enterprise), McAfee Policy Auditor, McAfee Remediation Manager, and McAfee ePolicy Orchestrator, which serves as a central management console for the entire suite. This portfolio, taken as a whole, provides a rich set of security compliance orchestration functions. These functions have until recently not been well integrated, but McAfee has recently released new versions of several portfolio components, which improves the level of integration both within portfolio products and with third-party offerings.

Table 5 synopsizes the capabilities of the McAfee portfolio.

Orchestration element	**Product capabilities**
Knowledgebase of regulations and control standards	McAfee Risk and Compliance Manager's PolicyLab provides out-of-box support for a number of regulations and standards, including SOX, HIPAA, Gramm-Leach-Bliley Act (GLBA), and Federal Information Security Management Act (FISMA), and for a variety of control standards including ISO 17799, NERC, FERC, CoBIT, and various NIST standards. The solution provides a map between high-level requirements and controls that must be assessed for conformance to the requirements.

Creation of organizational security policy	PolicyLab allows creation of organizational policies from scratch, but enforcement rules must be hand-coded to map assessments to policies. McAfee provides services support and training for policy authoring.
Importation of organizational security policy	PolicyLab allows importation of existing natural-language policies, but enforcement rules must be hand-coded to map assessments to policies.
Default controls	Default controls and related technical checks are provided in accordance with the knowledgebase. The product supports both automated controls and a workflow for attestation of manually audited tasks such as clean desk policies, locked doors, and so forth.
Technical-infrastructure assessment	McAfee Risk and Compliance Manager provides a sizeable list of supported connectors to assess the status of IT systems. Both McAfee scanners (including McAfee ePolicy Orchestrator, McAfee Vulnerability Manager, and other McAfee products) and third-party scanners can serve as sources for assessment information.
Non-technology assessment	The portfolio provides a workflow and manual inputs of non-technology processes for assessing risk outside of IT. The capability is not as robust as the self-assessment features in some risk assessment point solutions.
Security compliance tracking	Mapping from external requirements to policies and then to controls creates requirements traceability. When assessments are conducted, compliance teams can discern where gaps lie at the infrastructure, control, policy, or requirement level. Manually audited compliance tasks can be tracked using McAfee Risk and Compliance Manager.
Feedback/reporting	McAfee Risk and Compliance Manager relies on a “people, process, and technology” approach to compliance assessment. The product combines vulnerability, threat, and configuration data from a variety of sources to create risk and compliance assessments. It supports graphical dashboards and management reports that allow views of policy violations, compliance deficiencies, and risks; the dashboards also allow users to assign responsibility for remediation tasks and to track and report on remediation progress.
Resolution	McAfee Risk and Compliance Manager's built-in workflow or help-desk integration (specifically with Remedy) can help facilitate manual resolution of problems. Risk and Compliance Manager integrates with McAfee Remediation Manager for remediation of identified issues.

Table 5: *McAfee Solution Features*

Modulo

Founded in 1985, New Jersey- and Brazil-based Modulo (www.modulo.com) is Latin America's leading risk-management vendor. The company serves large enterprises and small and medium-size business (SMB) customers, with particular focus on banking, telecommunications, government, and heavy industry.

Modulo Risk Manager 5.1 provides a knowledgebase which supports simultaneous compliance with multiple regulatory and control frameworks, including CobiT, ISO 27001, HIPAA, Fiscal Operations Report and Application to Participate (FISAP), Federal Information Security Management Act (FISMA), NIST 800-53, PCI Data Security Standard (PCI DSS), and Department of Defense Information Assurance Certification and Accreditation Process (DIACAP). The product integrates risk management with business continuity management and incorporates (in addition to a compliance remediation management workflow) an incident management facility.

Modulo's key differentiators are strong integration of risk management and business continuity functionality, and support for assessment and remediation of risks other than IT security risk. The product incorporates extensive support for survey-based assessment of many types of risk including natural hazards, environmental hazards, disease, and others. The product includes a knowledgebase, derived from the company's 25-year experience in risk management and compliance, with over 11,000 controls and 4,500 automated risk information collectors. Assessments can be carried out through surveys conducted using mobile handheld devices, for which Modulo Risk Manager provides native support. The product allows users to view risks from many different perspectives, including organizational, role-based, and geographic views.

Key components of Modulo Risk Manager include:

- **Knowledgebase:** Modulo has built a knowledgebase which maps multiple regulatory and control frameworks onto a collection of 11,000 discrete controls.
- **Risk Assessment:** The product includes more than 3,700 automated collectors which capture status from a wide variety of target platforms and applications. The product also includes a set of prepackaged manual surveys for collecting information which cannot be automatically collected. A risk scoring algorithm takes into account probability of incidents, impact of incidents, and business relevance of the affected system. The risk assessment methodology proceeds top-down, (from business processes to applications and finally to assets) to facilitate prioritization of the most business-relevant and high-impact risks.
- **Reporting:** The product generates a set of customizable risk assessment reports which can be mapped to an organizational chart to facilitate mapping of risks to business entities and responsible parties.
- **Incident Management:** The product provides an integrated remediation workflow manager which consolidates remediation actions required by multiple regulations and control frameworks, routes remediation actions to responsible individuals, tracks progress of remediation actions, and maintains evidence of actions taken. Incident management is also supported by this component.

Modulo Risk Manager is licensed based on the number of servers monitored. Enterprise licensing is also available; an average deployment costs about $40,000 annually.

Table 6 summarizes Modulo Risk Manager's features.

Orchestration element	**Product capabilities**
Knowledgebase of regulations and control standards	Modulo Risk Manager provides a database of 11,000 discrete controls mapped to a variety of regulations and control frameworks, including CobiT, ISO, HIPAA, FISAP, FISMA, NIST 800-53, PCI DSS, and DIACAP.
Creation of organizational security policy	Organizational security policy is created in a top-down fashion based on prioritized (by severity, probability, and business relevance) risks to environment, people, processes, and IT assets. This policy can be derived from regulatory and control frameworks, and it can be customized to meet the needs of the individual customer.
Importation of organizational security policy	Controls can be imported based on specified control frameworks and regulations, and it can be customized based on the needs of the organization.
Default controls	Both IT and non-IT controls are included in the knowledgebase. Modulo Risk Manager provides especially strong support for non-IT controls.
Technical-infrastructure assessment	Assets are identified during product configuration. A set of more than 4,500 evidence collectors supports automated collection of risk status information about IT assets. There is also strong support for e-Surveys, including support for conducting surveys using mobile devices.

Non-technology assessment	Modulo places strong emphasis on the ability to identify and treat environmental, people, and process risks. Geospatial mapping integration allows risks to be displayed on a map of physical locations to allow identification and treatment of localized risks. The product includes a standard list of threats (human and nonhuman) and threat agents which are used as input to risk assessments.
Security compliance tracking	Survey results can be linked to control standards or regulations to reveal compliance per question or assessment area.
Feedback/reporting	Reporting is hierarchical: Risks to assets are indicated at the bottom of the hierarchy; they are then aggregated to display risks to applications, and these in turn are aggregated to display risk to business processes. Risks can also be placed on a Visio organization chart or on a geospatial mapping display.
Resolution	Mitigation efforts can be prioritized using an ROI analyzer tool. An integrated mitigation and incident workflow manager tracks mitigation activities and stores evidence of actions taken.

Table 6: *Modulo Risk Manager Features*

Symantec

Symantec's (www.symantec.com) acquisition of BindView yielded some policy-management and infrastructure-assessment tools that helped to fill out Symantec's compliance orchestration solution suite, which currently consists of Control Compliance Suite (CCS) 8.6 and an integrated security information and event management (SIEM) offering called CCS Security Information Manager 4.6. CCS's primary customers are large enterprises, though a significant number of SMB clients also use the product. The CCS pricing model incorporates charges per server, per monitored system, and per user seat. Enterprise licensing is available; an average deployment costs about $100,000.

Since the BindView acquisition in Q2 2006, Symantec has integrated the BindView technology into CCS to provide automated collection of information about system configuration, and it has extended CCS in several other ways. Symantec has added analytics to support a business-oriented compliance dashboard which displays summary compliance reports and evidence trend analysis. CCS 8.6 also integrates policy management with evidentiary feeds and procedural controls more tightly than in previous releases. CCS combines natural-language policy management with automated infrastructure-assessment to provide building blocks for security compliance orchestration.

The solution provides the following capabilities for users:

- Define and manage organizational policies
- Map organizational policies to controls implemented by infrastructure elements
- Collect evidence from technical components and some nontechnical processes that shows effective operation of controls
- Audit control gaps and user and machine account-entitlement deficiencies
- Remediate gaps through integration with ticketing systems such as Remedy
- Report compliance status and control deficiencies to responsible parties on a dashboard

Symantec's emphasis is on automation of auditing and monitoring across the enterprise, in order to facilitate continuous assessment against compliance mandates. CCS does provide support for distribution of manual surveys that are designed to allow asset owners to periodically review and approve user entitlements; however, support for other types of manual risk assessment surveys is not provided.

Symantec continues to integrate CCS with other elements of the Symantec security suite, most recently CCS SIM. Future integration with Enterprise Security Manager (ESM) is planned, which will add optional host agents to the assessment capabilities. Symantec CCS is the subject of the *Security and Risk Management Strategies* Product Profile document "Symantec Control Compliance Suite 8.6 and Other Vulnerability Management Products."

Table 7 summarizes Symantec's offerings.

Orchestration element	**Product capabilities**
Knowledgebase of regulations and control standards	The solution contains a comprehensive library of control statements that provides an abstraction layer between natural-language policies and underlying technical controls. For example, a user access policy might drive to three control statements: • Password-allocation process (i.e. how to give users their credentials) • Confidentiality awareness upon termination • Temporary-password uniqueness These control statements, in turn, have ties to infrastructure or processes that implement the control statements. Each control statement is linked to high-level regulatory and control standards such as HIPAA, FISMA, SOX, and GLBA.
Creation of organizational security policy	The solution supports creation of natural-language policies and supplies policy controls recommended for compliance with regulatory and control standards; separate standards can be created for a variety of supported platforms, including Windows, UNIX, Linux, Oracle, and others.
Importation of organizational security policy	Existing policies can be imported and managed.
Default controls	Control statements are the nexus for controls in the product, linking policies, evidence collection and assessment, and compliance drivers. The product includes an innovative canvas that assists with controls mapping.
Technical-infrastructure assessment	Infrastructure control information and entitlement information can be assessed in three ways. First, the suite automatically collects assessment data and configuration standards. Second, the suite provides a generic adapter that can be customized and deployed to acquire information from third-party products which are not supported out of the box. Third, comma-delimited or Structured Query Language (SQL)-acquired data can be imported manually.
Non-technology assessment	The solution does not provide a self-assessment capability. Certain nontechnical controls may be assessable through periodic manual data import.
Security compliance tracking	Compliance is tracked largely through evidence collection and analysis against control statements.
Feedback/reporting	CCS now provides a robust compliance-reporting dashboard.
Resolution	CCS supports generation of tickets in external problem-resolution systems (including Remedy) and re-importation of status information from closed tickets. CCS also supports patch assessment and deployment via integration with a partner offering provided by Shavlik Technologies.

Table 7: *Symantec's Policy Manager Features*

Conclusion

Security compliance orchestration combines three activities: risk assessment, control management, and evidence generation. These activities must be performed by many people in most organizations, but the chief information officer (CIO) and chief information security officer (CISO) coordinate the activities. Security compliance orchestration solutions are maturing and can deliver real value. The so-called "IT-GRC" market is likely to consolidate around security compliance orchestration solutions, and then to integrate vertically by marrying these solutions to financial and organizational GRC solutions catering to the executive suite and to more specialized risk and controls management tools in the trenches of business IT departments.

Notes

[1] "FFIEC IT Examination Handbook." *FFIEC.gov*. Dec 2002. http://www.ffiec.gov/ffiecinfobase/booklets/information_security/information_security.pdf.

Author Bio

Bob Blakley

Vice President and Research Director

Emphasis: compliance, identity management, governance, authentication, privacy

Background: Bob Blakley is Vice President and research director for Burton Group Identity and Privacy Strategies. He covers identity, privacy, security, authentication, and risk management. Prior to joining Burton Group, Bob was former chief scientist for security and privacy at IBM and served on the National Academy of Science's study group on Authentication Technologies and Privacy Implications. Bob has served as general chair of the 2003 IEEE Security and Privacy Conference and as general chair of the New Security Paradigms Workshop. He is the former editor of the OMG CORBA security specification, and authored 'CORBA Security: An Introduction to Safe Computing with Objects,' published by Addison-Wesley. Bob is also editor of Open Group's Authorization API specification effect and currently holds more than 10 patents on security-related technologies.