

top 10 regulatory compliance

A Guide to Selecting a SIM Solution
for Regulatory Compliance



Effectively Address Compliance with a SIM Solution

Given the tremendous increase in government regulation over the confidentiality and integrity of sensitive information, it's no surprise that regulatory compliance topped the list of security initiatives with the highest priority, according to Deloitte & Touche's 2005 Security Survey.

Around the globe, laws like Sarbanes-Oxley, HIPAA, FISMA, PCI, Basel II and a host of others continue to push IT security management to take on more work with the same amount of resources. The bottom line is that organizations are required to place more stringent controls on regulated business processes and systems, and are also subject to a large burden of proof.

On top of general protective measures, public disclosure requirements have increased in complexity, requiring businesses to publicly report weaknesses in controls over financial reporting, consumer data breaches and other information loss, which can result in damaged reputation, loss of consumer faith and bad publicity. In some cases, disclosures have resulted in cancelled contracts, lost revenue and class action lawsuits.

To avoid negative consequences from non-compliance, organizations must demonstrate that their controls are effective and that their IT and business systems are robust enough to fend off fraud or serious attack. This requires the monitoring and management of millions of logs each and every day from dozens of data sources, including firewall, IDS, databases, operating systems, applications and directory services.

Log management for compliance has been a rude awakening for enterprise IT security departments. Even if organizations hired an army of security analysts, they still couldn't properly do the job of monitoring every log event. To address this problem, organizations are turning to Security Information Management (SIM) technology as a solution to automate the collection, preparation and analysis of this information.

While the right SIM technology offers great benefits to easing compliance requirements, organizations quickly find themselves not only immersed in understanding new compliance terminology, but new SIM terminology as well. The lack of standardized SIM terminology, combined with a morass of logs and ambiguous compliance requirements can lead to confusion as to what the right technology approach is based on organizational requirements.

ArcSight has developed the following list of evaluation best practices to assist organizations in making the right SIM choice for their compliance needs. This list has been compiled directly from the experiences of actual customers. These practices should be used as an integral part of your evaluation and selection process.

10

A Compliance Program Should Address Your Unique Needs

There are many confusing and contradictory messages about what really needs to be done to achieve compliance. While it may be tempting to search for oversimplified solutions and check-the-box approaches that may help you fulfill an audit point for one or two financial quarters, it is really in your best interest to find a solution that provides a long-term strategy for effectively dealing with regulatory compliance. Don't sell the problem short by thinking that all you need for compliance is log consolidation or real-time monitoring or compliance reporting. The simple fact is that no instant solution exists with regulatory compliance. You need a solution that takes into consideration the uniqueness of your organization including how you exchange information, what technology architecture you use for your networks and systems and how your IT security organization is arranged. Prior to and during the evaluation of a SIM solution, take some time to develop your own unique requirements set, including support for your customized policies and proprietary data sources.

9

Focus on the Regulated Business Process

When a vendor tells you it can help solve your compliance issues, your first question should be, how? To provide value for compliance, the solution must be able to map your technical information and log data to your regulated business processes, and then map your business process to your specific regulations. But first you need to understand which regulations apply to your business. Some regulations, such as Sarbanes-Oxley, require a control framework and detailed audit trail for the financial reporting process. But other regulations, such as SB 1386, do not stipulate the protection of information, but rather the public reporting of any unauthorized exposure of California residents' consumer data. This means you must take proactive security steps to ensure breaches do not occur. It's imperative to select a SIM system that not only offers a way to see compliance status as whole, but also allows you to separately review and gain an understanding of correlated technical events that deal with an asset threat for a specific regulation. SIM vendors should tell you up front how their product addresses different regulations and how they are delivering regulation-specific solutions for Sarbanes-Oxley, HIPAA, FISMA, SB 1386, PCI/CISP, ISO-17799:2005 and others.

8

Correlation Is Key to Compliance

Compliance requires active and immediate management of log events and the ability to capture processes now so you can prove compliance later. Log management is essential to compliance, but some SIM systems only provide reports of raw or slightly massaged data, which means you have to spend extra time and effort manually sifting through hundreds and hundreds of lines to find the exceptions. You need a system that is much more efficient—one that can intelligently and automatically do the heavy lifting of your report review process, as well as proactively identifying violations before they

significantly impact your business. Comprehensive correlation can churn through billions of lines of data and surface the policy violations and suspicious activity you need to know about for compliance requirements. A robust SIM solution will have both preconfigured correlation rules as well as customizable rules that meld to your compliance policies. With the right solution, you will be able to relate a massive number of technical events to actual compliance requirements and business processes. This will allow you to better understand and identify your biggest priorities in terms of security and compliance.

7

Compliance Should Improve Security

Compliance should not be viewed as a major headache that saps valuable time and resources, but rather an opportunity to help your organization implement a next-generation security program. Compliance is a hot-button issue these days, maybe even more so than security. Unfortunately, this can lead to a focus on a compliance “check the box” approach to initiatives and technology purchases rather than a focus on improving the security of the regulated information. Remember, you may only get this budget once, so choose a system that enables you to protect the business and achieve compliance at the same time.

6

Use Your Consulting Dollars Wisely

Look for a SIM system that can be deployed quickly with out-of-the-box intelligence and collection capabilities to deliver immediate results. Some solutions are much easier to deploy and require only limited consulting services because they include easy-to-use authoring tools and support a long list of third-party products for event and audit log collection. When comparing SIM solutions, take time to understand what minimal amount of consulting services are required in the initial phase of deployment. This will help to ensure that you use your consulting dollars on building better policies and procedures for log management and not simply on making the product operational. This allows enterprises to use their resources to improve their overall security program instead of grappling with basic deployment issues.

5

Understand the Value of Vendor-Developed Compliance Solutions

People new to the world of IT compliance will quickly be exposed to a wide mix of letters and numbers such as COBIT 4.0, ISO 17799:2005 and COSO. While these control frameworks provide high-level guidance for IT security, they alone do not provide adequate guidance for granular technical practices such as log management. It is important to understand what approach your vendor has taken with pre-developed compliance solutions, the granularity of the methodology that has been used to ensure best practices and the level of research that the vendor has applied to their compliance solutions. The best solutions for compliance will be based on more detailed standards, such as NIST 800-53, which objectively lay out common security control definitions and compliance criteria for IT.

4

Place a Premium on Data Collection

Proper data collection is essential to any compliance program. The system must be able to collect all the data from events that are relevant for compliance purposes. It's important that vendors support a large number of data sources and can effectively collect and process log data. SIM solutions addressing compliance need to collect log events from perimeter security devices in addition to an ever-growing list of internal and system level controls including applications, databases, directories, OS logs, physical building security systems and more. Also, evaluate the vendor's custom connector development capabilities. Ask

about custom connectors that are being used at customer sites and the number of customers that are currently developing their own connectors with the provided toolkit. Lastly, validate that standard connector features are available for custom developed connectors. Some vendors only offer simple parsers under the guise of a complete custom connector development environment. This simplification has been known to severely limit custom-developed connector performance and capabilities.

3

Make Sure Your SIM System Can Adapt to New Compliance Requirements

Compliance best practices and audit procedures are immature. That's because many regulations are still evolving and we don't know what they will look like several years down the road. Unfortunately, organizations are faced with an element of uncertainty when it comes to complying with existing laws—not to mention new regulations that continue to be introduced by both government and private industry. This creates a strong requirement for an easily adaptable SIM solution that can grow with your organization and meet any future regulatory requirements and continually increase automation. It is not just

compliance requirements that are changing, but also threatscapes and vulnerability status. Even the very nature of your business may be in flux due to acquisitions or unforeseen financial events. You need a SIM solution that is flexible and agile enough to deal with these changes. Carefully research each vendor's ability to customize every resource, including access control, notification groups, reporting, correlation rules and associated actions. In addition, you will need to bring in more data sources as your compliance practices and requirements evolve. It is important to understand the depth and breadth of supported products offered by the SIM solution as well as the maturity and architecture of any customizable connector kits offered by the vendor.

2

It Is Not Enough to Be Compliant, You Must Also Prove It

It's not just the "doing" that makes a company compliant—it's the "proving" to auditors. When evaluating a SIM system, ensure that workflow and the richness of the audit trail are carefully evaluated. A common audit point includes proving processes have been followed and controls have been executed. The ability to execute and report on a closed loop workflow will go a long way to gaining the greatest efficiency from your SIM solution. In addition, the ability to retrieve information from the audit trail in an ad-hoc manner is critical. Investigations, review and addressing audit points requires the need for in-depth data retrieval and mining capabilities.

1

Compliance Is Not a One-Time Event

Compliance is an ongoing activity. It is something we are constantly doing, and not just something we tackle once a year to satisfy auditors. When selecting a SIM solution for compliance, take time to understand exactly how each product can make your department more effective and how each product can help you proactively manage your compliance efforts on an ongoing basis. Because these practices will continually build themselves into daily departmental activities, making certain that you gain efficiency for both security and compliance objectives will lower your long-term overhead and prepare you for the changing road ahead.

Start

Get Started Today

ArcSight offers an enterprise-class security information management and compliance solutions that can cost-effectively address a broad range of compliance requirements. We welcome you to test our family of compliance products head-to-head against any on the market. Our account executives can provide more details that address your specific criteria, show you a product demo and provide a trial for an in-depth look into our solution. It's no coincidence that leading publications recognize ArcSight ESM for its superior flexibility, functionality, scalability and ease of use. For help with your enterprise security management and compliance needs, contact ArcSight at info@arcsight.com, call (408) 864 6150 or visit us online at www.arcsight.com.

Now

About ArcSight

ArcSight is a leading provider of security and compliance solutions that intelligently identify and mitigate business risk by delivering a centralized view of enterprise-wide events across heterogeneous infrastructures. This real time and historic view into external attacks, insider threats and regulatory compliance provides enterprises, MSSPs and government agencies with the intelligence and response capabilities required to effectively protect their businesses.

ArcSight, Inc.

5 Results Way, Cupertino, CA 95014, USA

Corporate Headquarters: 408 864 6150

EMEA Headquarters: +44 870 351 6510

Asia Pac Headquarters: 852 2166 8302

Email: info@arcsight.com

www.arcsight.com