

Ease the compliance burden with automation

by: [Richard Mackey Jr.](#)

Issue: [May 2009](#)

Just as a check-box approach to compliance doesn't guarantee security, good security practices aren't necessarily enough to meet regulatory compliance requirements.

The point is, you may actually achieve a substantial degree of data security if you see securing access to sensitive information as an exercise in operational security. But, that alone won't pass muster when the auditors come in.

Virtually all regulations and contracts, from HIPAA to FFIEC guidelines to the PCI DSS, require documentation, audited requests and approvals, logging, and review of all the operational activities that companies engage in to protect the particular regulated information. Many organizations find this additional dimension troublesome and underestimate the added organizational and process burden that comes with it.

Most regulations and regulatory guidance are carefully written to avoid suggesting particular technologies, and none provides any requirement for automation of your compliance activities. However, for all but the smallest organizations, the "paperwork" associated with compliance can become unmanageable without some technological help.

In fact, technology can improve an organized approach to workflow, documentation and verification to meet compliance requirements common to many regulations.

COMMON REGULATORY REQUIREMENTS

Regulatory compliance requires organizations to be able to *prove* that controls they have in place: The mandates are:

- Effectively protect the regulated information or operations.
- Are enforced consistently.
- Are inspected for correctness and integrity regularly.
- Provide the necessary transparency to prohibit circumvention.

These requirements put pressure on organizations to manage identity and access control effectively; monitor the state of systems to ensure that vulnerabilities or configuration changes do not degrade their trustworthiness, and ensure that some disinterested party is charged with watching all the use and administration of the systems.

Fortunately, regulations have many similarities in the kinds of controls they require. While they may call these requirements by different names, the regulations are trying to achieve the same basic goal: protect the confidentiality, integrity, and/or availability of a particular class of information. For HIPAA, it is health information. For PCI, it is payment card information. Regardless of the specifics, it pays to have a set of rules of thumb to allow all your compliance activities to benefit from the commonality.

Following these is at the foundation for meeting regulatory requirements:

Identify regulated information. HIPAA requires that organizations identify all systems where electronic protected information exists and ensure that all required controls are in place on the those systems. Similarly, PCI requires that companies clearly define their cardholder data environment and base all control requirements on how that area is cordoned from the rest of the company.

In any event, organizations need to erect barriers to segregate regulated information from the rest of the environment. Technologies such as firewalls, intrusion detection and intrusion prevention are the main tools used to establish and enforce the separation between environments. Of course, once these mechanisms are in place, they need to be monitored.

Determine who has authorization to access the regulated information. All regulations require organizations to maintain tight controls over the people who are allowed access to protected information.

This means more than access control. It means ensuring that supervisors and information owners are involved in the approval access and that they only provide access to appropriate individuals. It also means that there must be records of the entire approval process and account creation.

While this process and the records associated with it can be captured manually, even smaller companies find it difficult to install the discipline required to do it well. This aspect of regulatory compliance is one of the main reasons why so many companies are turning to identity and access management (IAM) products to gather approvals, notify interested parties, capture audit logs, and even automate account creation and disablement.

Make sure that only appropriate people have access to the regulated information. Once accounts are created, they need to be recertified periodically by the same people who approved the creation of the account. Even when organizations are good about requiring and capturing account creation, many do not do a good job of carrying out the periodic checks.

This is another area where IAM systems are valuable. They can help you automate the process recertification, reminding supervisors and information owners periodically that checks and approvals are necessary, and capturing the approval process.

Monitor who has accessed the regulated information. Even if we know who *can* access the information, the question is "who *has* accessed the information?" Regulations call for capturing and monitoring access to protected data.

Monitoring does not mean saving the activity to log, only to be unearthed in the event of a suspected incident. It means sorting through the information captured and looking at the access that authorized (or unauthorized) individuals and applications have had to the information. This task is almost impossible without the help of technology to both gather and reduce the logs to a consumable format and size.

Know and monitor the state of the systems and the network in which they exist. This "rule" is relatively vague, but understanding state is a broad area that needs to be adapted to the particular regulation. The idea here is that you need to know the current state of the operating systems, applications, networks, and any associated vulnerabilities these components may have. Examples of state are network configurations, operating system versions and configurations, and device firmware versions.

Keeping these points in mind when designing your compliance program can help you stay ahead of regulatory and contractual requirements. This is because regulations differ to a significant degree on the specificity of technical controls. PCI, on one hand, is relatively prescriptive in that it discusses protocols, vulnerability management practices, password standards, and the requirement for dedication of a single system to a single function. On the other hand, HIPAA, GLBA, and others refer only to best practices in most of these areas. By staying on top of the configurations and state of all your systems and networks, you will be able to adapt to requirements as they become more explicit. For example, if you track the versions and vulnerabilities of software you have deployed, you can more easily adjust your patch frequency to match the requirements of prescriptive standards like PCI.

There are a variety of technologies to help track and control the state of your systems. Vulnerability management and configuration management systems are the most popular security tools designed to help organization meet compliance requirements.

AUTOMATING IDENTITY MANAGEMENT

One critical element of compliance is controlling access to regulated information. However, before you start choosing technology to manage access, it pays to step back from the technical aspect of access control and think about it conceptually.

Almost every regulation makes the point that only people with a business requirement for access should be given access. Determining who should have access is the job of information owners, supervisors, and information custodians.

So, by stepping back, we see that the first consideration in assigning and controlling access is establishing who is responsible for making those decisions. These responsible parties establish the rules for guiding the assignment of organizational roles and ultimately all access controls.

These rules form the basis of your access control policy and, in and of themselves, are a critical part of compliance. The organizational structure, combined with the access control policy, is what is referred to as governance. Unfortunately, there is no technical mechanism that can sort out who should have access; it is a process driven by people.

Even when you have the high-level rules and structure defined, there is more work to do: You need to apply the policy to your entire organization. Basically, this means identifying which people take on roles of supervisors who approve access, the administrators who are responsible for custodianship of the systems housing the protected information, and what approvals are necessary to allow particular types of access.

IDENTITY MANAGEMENT THE HARD WAY

Once you go through this process, you are at a point to decide what mechanisms you will use to manage it. You can certainly capture the approval workflow in a spreadsheet or database and track all the activity manually, but that's both inefficient and prone to error.

Another common--but unacceptable--practice is to advise the various parties of their responsibilities and let them manage the approval process on their own. In this model, the logging for the requests, approvals, and provisioning is typically left to the email system, and it is unlikely that anyone can oversee the process.

Auditors will find multiple compliance problems with this approach: There is no systematic enforcement of the process and no guaranteed record of the requests and approvals. Finally,

even when all the requests and approvals are captured, the email system may not be controlled to the extent that it would allow an auditor to reliably follow the events that led to approval.

A third way to attack the problem is to leverage a trouble ticketing system. This can be an effective way of requesting, approving, and tracking requests for access and--if configured appropriately--provide some level of reporting. This approach is often a good, and relatively inexpensive, first step in automating the required request and approval workflow. However, ticketing systems are not purpose-built for tracking identity management operations, so they may not have a number of features that systems design for the task would.

MAKING IDENTITY MANAGEMENT WORK

Many organizations come to the conclusion that the complexity of the task and the requirement for an verifiable audit path justifies the purchase and deployment of an identity and access control system. These systems are not simple to deploy, and they are not cheap, but they can help meet several requirements from many regulations. They can also help organizations improve their security in the process.

Identity and access management systems are really two systems that are typically packaged together. The first is identity management, the process of creating accounts for people (and other entities, such as services). IAM systems also handle access control which takes the identities and assigns privileges or authorization to access resources. Access management incorporates both users (or principals) and resources.

One of the reasons these systems have become so popular is that they support the administration of identity and access across different identity stores, applications and, in many cases, multiple identities for the same people across different systems. In other words, the promise of these systems is that they will eventually allow organizations to have a single centralized service to manage "all" accounts.

While identity management and access control are different jobs, they share many common elements. Both require:

- An auditable approval workflow, reporting of state (accounts and access).
- Notification of changes.
- Integration with underlying technologies, such as operating systems, authorization systems, directories and devices.

All of the leading identity and access management systems support integration with Windows, UNIX systems, Active Directory, LDAP, and much more. This integration allows these systems to support automatic creation and deletion of accounts and automatic changes to authorization. The leading products are also extensible, so you can integrate your own applications and systems into the mix.

While this automation capability is very useful, the two most important IAM features for compliance are the abilities to specify a strict approval workflow and audit those approvals. This allows you to demonstrate to an auditor that you have a formal identity management and access control policy and a mechanism to enforce it.

The systems orchestrate the entire process from notification through the capturing of all approvals (or rejections). They can even remind you periodically that account and access recertification is necessary and capture the activity in logs for auditors.

As an added bonus, these systems can automatically recognize and prohibit role conflicts. For example, it is important for many organizations to ensure that certain types of transactions be requested and approved by different people to provide transparency and avoid fraud. While defining these roles and conflicts is a manual process, identity management administrators can define the relationship between the roles, so conflicts can be automatically detected and prevented.

AUTOMATING STATE MANAGEMENT

State management is a broad area that includes system and network configuration management, vulnerability management, and monitoring. Every regulation requires you to track and control the state of all systems, networks, and devices in the target environment.

Effective state management can be accomplished with a variety of manual processes. Organizations often maintain detailed specifications of configurations of all systems and devices in documents and spreadsheets, and conduct periodic manual audits.

The larger and more complex your environment, the more cumbersome this manual process can be and the more automation can help. Many products that can be purchased separately or as parts of an integrated suite provide automated management of state. They tend to be organized around two functions: configuration management and vulnerability management:

Configuration management and monitoring. Configuration management systems allow you to specify and monitor configurations of services, ports and protocols. Some products require agents to be deployed on the monitored systems, some monitor remotely, and some determine configuration by passively monitoring network traffic.

Configuration monitoring tools can be programmed to look for behavior that violates compliance requirements. For example, for PCI DSS compliance, they can look for insecure protocols such as rsh and Telnet, or the presence of open ports in the cardholder data environment. Vendors continue to develop regulation-specific templates to scan for violations.

Vulnerability tracking and patch deployment. Vulnerability management systems determine the versions of operating systems, services and applications and match them against published vulnerability announcements. They require a subscription to a vulnerability tracking service and can substantially reduce the amount of work you will need to devote to scouring vulnerability announcements and comparing versions and vulnerabilities.

These products also provide dashboard displays of systems, versions, vulnerabilities, and the severity of vulnerabilities on your systems. Your network zones will appear as an array of green, yellow and red boxes depicting the severity of vulnerabilities on each system. Some of these products also calculate risk based on asset value. For example, a system running a vulnerable Web server that is exposed to the Internet poses a higher risk of compromise than one only exposed to your corporate network.

Vulnerability management systems can be integrated with patch deployment tools to automate the distribution and application of patches that address vulnerabilities. While this type of automation can be a time saver, it doesn't cover one of the most critical manual steps in state management: change control. Let's examine this further.

Recognizing state problems is the first step in good management. Bringing the systems into technical compliance is a process that requires discipline, thought and a clear audit trail. Vulnerability management tools can help, but the entire process can never be completely automated.

Once a vulnerability is identified, good practice and most regulations require that you conduct a risk assessment to determine whether there is more risk in allowing the vulnerability to exist or patching the vulnerability immediately without adequate testing. Business and technical representatives must weigh factors such as planned downtime, potential outages and software incompatibility against the likelihood that the vulnerability will be exploited. The business may be willing to accept the risk of compromise for some period, may require additional compensating controls such more monitoring, or may even accept the risk of downtime if the risk of an exploit is too great.

This kind of risk-based approach can be problematic if you are subject to PCI, which requires that systems be patched within a specified time period. However, you may be able to convince the assessor that your acceptance of risk is appropriate if you can provide evidence of the risk assessment, the reasoning behind your decision, and compensating controls that achieve an equivalent level of risk mitigation. The combination of a clear understanding of your state with good risk management and configuration control will go a long way with any auditor.

If you are structuring your security practices to comply with HIPAA, identity theft laws, PCI or other regulations, it pays to focus on the fundamentals like identity and access management and state management. Both these activities require well-defined processes and organizational discipline, but they can also benefit from appropriately applied technology.

If you create the right organization and policy and apply systems like identity management and vulnerability management technologies prudently, you can not only ease your day-to-day operations, but significantly reduce the risk of failing an audit and reduce the effort needed to pass.

Richard E. Mackey, vice president of SystemExperts. Send comments on this article to feedback@infosecuritymag.com