

Three Step Approach to Compliant Log Management

by J.J. Thompson

27-JAN-11

It's all about the data. What data do you care about, where is it, how are you protecting it, how are you monitoring access and use of the data, and how are you monitoring the controls in place to protect the data? Finally, how do you identify anomalies in use behavior or control performance? The answers to these questions drive your initial business and compliance requirements (Step 1), then evaluate the requirements and internal constraints to determine if your organization has the resources to manage the tools internally or if you need to evaluate managed service providers (Step 2). Finally, the evaluation of potential vendors will be driven by the aforementioned requirements and internal constraints to determine the most adequate end-to-end solution both today as well as over a period of time, usually one to three years (Step 3).

Step 1:

What data do you care about? This should be driven by your compliance requirements, business metrics, internal controls, and any customer or contract requirements.

Where is it? Conduct a mapping between the "business friendly names" of the data that is in-scope to the assets that the data resides on (or passes through).

How is the data protected? Now that you know the data that needs monitoring, the locations where the data resides, and where it passes through, now identify the controls that prevent an unacceptable result (mis-use, corruption, loss, etc.) or detect when it takes place through the end-to-end process or life cycle of the in-scope data from creation or receipt through use and destruction. The resulting alerts or logs from the technical controls utilized to protect data at various stages of the process need to be monitored.

How are anomalies detected? Using the outputs from above, evaluate the data (logs, alerts) that will be created to determine what the normal use / normal logging and alerting levels look like. This baseline should take place over a period of time until an average use pattern can be determined.

Step 1:

What data do you care about? This should be driven by

your compliance requirements, business metrics, internal controls, and any customer or contract requirements.

Where is it? Conduct a mapping between the "business friendly names" of the data that is in-scope to the assets that the data resides on (or passes through).

How is the data protected? Now that you know the data that needs monitoring, the locations where the data resides, and where it passes through, now identify the controls that prevent an unacceptable result (mis-use, corruption, loss, etc.) or detect when it takes place through the end-to-end process or life cycle of the in-scope data from creation or receipt through use and destruction. The resulting alerts or logs from the technical controls utilized to protect data at various stages of the process need to be monitored.

How are anomalies detected? Using the outputs from above, evaluate the data (logs, alerts) that will be created to determine what the normal use / normal logging and alerting levels look like. This baseline should take place over a period of time until an average use pattern can be determined.

Notable Compliance Drivers for PCI

Vulnerability Assessment

- 6.2 Identify newly discovered security vulnerabilities
- 11.2 Perform network vulnerability scans quarterly by an ASV

Intrusion Detection

- 5.1.1 Monitor attacks (including zero-day) not covered by Anti-Virus
- 11.4 Maintain IDS/IPS to monitor & alert personnel, keep signatures up to date

Log Management

- 10.2 Automate audit trails
- 10.3 Capture audit trails
- 10.5 Secure logs
- 10.6 Review logs at least daily
- 10.7 Store logs for 1 year

Delivering What Matters: Three Step Approach to Compliant Log Management

Step 2:

What is your budget? Hopefully, when you initiated this process, you identified the average costs associated with the cost drivers of this initiative including planning, analysis, design, and implementation and did not forget the training and people costs associated with SMEs to manage the implementation and on-going management of the tools, nor did you forget the on-going maintenance and log storage costs.

What people are needed? Throughout this process, from inception to implementation and on-going management, one of the biggest areas where the effort can fail is by not having team members who are more than capable of understanding the business processes, compliance requirements (and auditor perspective), as well as the technical knowledge and ability to apply the results from the tools to provide alert triggers, business intelligence, and control performance metrics to the appropriate stakeholders. Without the right people, this initiative will fail. Determine if you can staff this internally or if you need to hire a contractor, employee, or if a consulting firm or third party Managed Services Provider will be needed to realize success for the initiative.

Step 3:

Document the constraints and requirements noted above. The requirements should be vendor agnostic and written more as an engineering requirement initially so that the requirements are not shaped to a vendor, skewing evaluation results. ie: the solution shall provide the ability for log data to be stored securely, in compliance with HIPAA, PCI, and SOX requirements.

Research vendors. Determine which vendors are most likely to fulfill your requirements and invite them to pitch you on their solution. Provide your engineering requirements and allow them to write various versions of the RFP for you. You can then combine the components from the RFP to form your RFP and do less legwork. Additionally, ask the vendors to map to your engineering requirements in a table to simplify side-by-side vendor-to-vendor comparisons.

Identify cost drivers. Make sure to understand how much storage is required per event (or better yet, groups of 10,000 to 100,000 events. Compare this to your existing records of average events per host, device, etc., to determine what your log storage requirements will likely be over a period of time. Identify the costs of training, re-training, on-boarding, working with consultants, or third party

MSSPs through the lifetime of the contract, license agreement, or expected lifetime of the regulation or valid period for the business requirements. It is likely that the period would not reasonably exceed 3 years.

Remember that pre-packaged will still = time. Vendors providing pre-packaged reports and alerts (such as for HIPAA, PCI, FISMA, NERC, COBIT/SOX, ISO27001 and the more general ITIL) can save you a lot of time, but do not eliminate the need for a person to evaluate how the log packages provide data that is useful based on your requirements.

Quick Notes on Cloud Logging & Security:

The cloud does not solve your problems and does not change the need for data centric security controls. Conduct due diligence for your cloud providers. Collecting SAS70 type II's is not enough. You need to review them against your requirements and compliance needs to verify that the provider's controls are adequate. Implement well accepted security best practices, which also defines expectations for 3rd party providers. Check out Cloud Security Alliance and BITS Shared Assessments. Leverage appropriate technologies to your advantage (Log Management, SIEM, virtual network activity monitoring, etc.) Make sure you have the ability to monitor and correlate information in the cloud; this includes making sure 3rd party providers offer access to required management and security functions.

How We Help Companies Succeed

Rook provides IT Risk Advisory services that support log management initiatives for organizations at various phases of maturity in their overall monitoring program. Whether your organization is dealing with an emerging regulatory compliance effort, or if you are looking to improve upon your existing program, Rook can provide the methodology and team members with the technical, audit, and management strategy expertise required for success.

Readiness Review - We assess the current state of controls to the desired state of controls to support management strategy, sales enablement, or general compliance efforts. Whether for HIPAA, HITECH, ISO 27002, SOX, PCI, GLBA, FISMA, NIST, or a myriad of other regulations and standards, we provide the knowledge and experience necessary to identify the approach best fit to your organization and prioritized to guide compliance efforts.

Requirement Definition - Working closely with your management and technical teams, we provide experienced professionals who identify the business and technical requirements necessary to a successful log management initiative.

Data Mapping - Whether the scope is known or unknown, we work closely with process owners, system owners, and data owners to determine the data flows for critical and sensitive data, then identify the infrastructure that is in scope based on the data location when at rest, in use, or as it traverses the network.

Control Identification - When the data mapping is complete and in-scope infrastructure has been identified, controls are identified throughout the process. Identified controls are compared to the desired future state in a gap analysis, and then gaps are documented, and prioritized based on the requirements, budgetary constraints, existing technology, and human factors such as knowledge and internal politics.

Vendor Selection - Requirements are utilized to create Engineering Requirements and a resultant vendor selection matrix. Vendors are reviewed to determine adequacy based on analyst guidance, past experience, internal contacts, and marketing materials. Vendor capabilities are documented, analyzed, the proposal process managed through vendor selection, contract evaluation, and project plan creation.

Health Check - The existing implementation is reviewed to determine if the end-to-end process, team members, and technology (comprising of the Monitoring Program) is operating at optimal efficiency. Areas for improvement are identified, technical configurations are updated, process improvements are managed, documentation updated, and training conducted.