

## Automating Compliance Monitoring and Reporting

Whether it is PCI, CoCo, SOX, HIPAA or MIFID, overcoming the next compliance 'hurdle' can be an enormous drain on already overstretched IT resources.

As well as being highly disruptive, compliance mandates, and the compliance auditors who scrutinise organisations against them, place extraordinary demands upon logging, reporting and auditing processes. Frustratingly, these will be different for every compliance requirement and, because there are few hard-and-fast guidelines about what really constitutes compliance, they will emerge in unique response to an organisation's business apparatus.

The resulting mish-mash of compliance management systems, controls and templates can take an age to construct, cost a huge budget to maintain, and consume significant resources to develop and improve. To alleviate these problems, and improve the ongoing compliance status of your organisation, automation of these processes is essential.

### AUTOMATED IT RATING: 4.4

This advisory describes the process and impact of automating audit, log and report management to meet compliance.

- **Situation Analysis (Before & After Automation)**
- **The Business Criticality of Automating Compliance Monitoring and Reporting**
- **Automation Impacts**
  - - Running Costs
  - - Time/Labour
  - - Space & Power
  - - Decision Making
  - - Uptime
- **Implementing Automation**
- **Q1 Labs Solutions**

### Situation Analysis

#### Before Automation

- Compliance can be seen as a burden with a tight deadline and therefore meeting the standard is viewed as the only end-game. This is to the detriment of security objectives, as the IT department is in danger of considering 'being compliant' the same thing as 'being secure'.
- IT professionals are negative and fearful about the compliance process, leading to team morale problems.
- Individuals are forced to abandon other projects at short notice in order to rapidly respond to an urgent, poorly planned compliance validation request.
- Each requirement of the compliance mandate is painstakingly interpreted and implemented using a manual process.
- Where there are multiple compliance mandates, the organisation unwittingly duplicates processes in the haste of making certain they are covered all ends up. Any new compliance requirements must be learned and implemented from scratch, often by separate groups in a company, blind to the efforts of their peers.

#### After Automation

- - Meeting compliance is viewed as a positive process, and the organisation is empowered to proactively identify and attain compliance and quality-standards based certifications. Because compliance validation can be achieved on the road to better security there is no complacency about meeting compliance requirements equating directly to 'being secure'.
- The prospect of urgent and disruptive compliance-related impacts on the IT department is removed, and activity planning can remain focussed upon strategically valuable projects.
- The process of mining, interrogating and presenting specific audit/log/report information is straightforward and intuitive, and based upon accepted control frameworks and templates. Manual intervention is eliminated.
- Intelligence for compliance management is centralised, which promotes the most efficient use of data. This eradicates unnecessary duplication of effort, and enables the organisation to meet future compliance goals more easily based upon what it has learnt to date.

## The Business Criticality of Compliance Monitoring and Reporting

All compliance mandates are underpinned by a monitoring requirement to prove and record individual activities through acutely specified and granular logging, auditing and reporting. Without these audit safeguards, no regulatory standard would ever been signed off by a QSA (Qualified Security Assessor) or auditor.

However, these aspects of compliance are often the most resource-intensive to establish and the most prone to failure. Collecting and then making sense of, millions of pieces of data (and under threat of such damaging penalties) is a significant challenge. The only course is to implement a system to automate and manage these processes, ensuring budgets and resources are used efficiently, and that the goals of compliance and better security are met rapidly and effectively.

## Automation Impacts

### Running Costs

HIGH 😊

The biggest cost saving that can be achieved through automation relates to the amount of time freed up by stripping away unnecessary manual processes and duplications.

In addition, some solutions can provide additional benefits by way of their embedded compliance intelligence. For example, a comprehensive tool-set of rules and thousands of proven report templates which are known to satisfy compliance auditors with specific regard to individual regulatory standards.

Moreover, some solutions are converged with other related capabilities that, when deployed, do the job of four 'point product' solutions, for around the same cost as one. This illustrates the importance of developing compliance reporting strategy alongside other IT management must-dos such as log management, network behaviour analysis, and security event and information management (SIEM).

## Time/Labour

HIGH 😊

Automation of compliance monitoring and reporting means dramatically less fire-fighting, especially at short notice. This enables significant reallocations of planned and unplanned resources. It also positively impacts the morale of IT professionals within the team who no longer dread the processes involved in attaining compliance, and who have more of their time available to pursue strategically valuable initiatives, like better security.

Automation also lowers skills barriers, meaning it can be carried out by a number of people without the expertise needed to do it manually.

The best automated systems come pre-loaded with easy to follow configuration wizards, minimising time and expertise required to implement and fine-tune.

## Space/Power

MEDIUM 😐

While its overall potential efficiencies are outstanding, this automation strategy has a limited overall impact on space and power in the datacentre. However, in the event that the automation occurs as part of a consolidation strategy that combines SIEM with log management, network behavioural analysis and compliance management, the space and power savings of rationalising four separate systems into one will create a beneficial space/power impact. Moreover, whatever is done in the physical datacentre can also apply to the 'virtual' datacentre without the requirement for additional product silos.

## Decision Making

MEDIUM 😐

Compliance is a critical driver for business; the requirements it places upon organisations are very real and IT departments must respond as a result. Ultimately compliance mandates attempt to drive a more efficient security operation in many areas particularly incident response.

Automation gives certainty to the decision-making process, enabling organisations to provide auditors and assessors with exactly the validation they require, presented in the format they need.

## Uptime

MEDIUM 😐

When regulatory bodies demand you to achieve a certain level of compliance, what they are really demanding is that for you to achieve a certain, *validated* level of security.

Any measure than seeks to do a better job of meeting compliance requirements, particularly if this gives rise to a more progressive and positive view of the compliance process, must be supporting that organisation to achieve an improved security posture.

## Implementing Automation

Implementation of tools to automate compliance monitoring and reporting can be accomplished almost immediately. Users find the process of fine-tuning their systems to their specific requirements easy and intuitive. Value can be derived from the first day of install.

Increasingly, smaller organisations are required to meet stringent and exhaustive compliance requirements, for example small UK councils endeavouring to attain GSX CoCo compliance. Automating technology is available which scales from this level of requirement right up to the huge multi-standard demands of the very largest organisations.

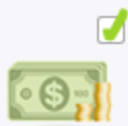
## Q1 Labs Solutions

This advisory has been produced with support from Q1 Labs, a global provider of high-value, cost-effective security management and compliance solutions. The QRadar family provides key technology underpinnings for a company's efforts to deliver security best practices as required by specific industry regulations. For more information, visit [www.q1labs.com](http://www.q1labs.com)

Click [here](#) to download the case study on Gordon Food Service

Click [here](#) to download the Meeting and Exceeding GSI/GCSx Compliance white paper

Click [here](#) to download the Business Case for PCI-Compliant Security Management solution note



### SLASH COSTS

- Cut management costs caused by unnecessary manual processes
- Create savings through freed up time
- One system performing the roles of four point products



### SAVE MAN-HOURS

- Eliminate significant reallocations of planned and unplanned resources
- Lower skills barriers allowing more people to possess expertise



### CUT SPACE/POWER

- Achieve power savings through rationalising systems
- Transfer benefits in physical datacentre into virtual datacentre



## BETTER DECISION-MAKING

- Achieve certainty to decision making process
- Ability to provide auditors with validation they require



## BOOST UPTIME

- Achieve validated level of security
- Gain a more progressive and positive view of the compliance process