Roadmap to SAP® Security and Compliance

Executives often view security and compliance management with a mixture of confusion and dread. The word itself encompasses so much: financial controls and reporting (SOX), privacy and data protection (HIPAA), technological deployment (HITECH), FDA regulations (21 CFR Part 11), and even national security (ITAR and EAR). Although security and compliance management in an SAP landscape has a very specific meaning, it often eludes decision makers.

The tragedy is that compliance rules are designed to protect your assets, security, clients and reputation. When they use the threat of civil and criminal liability, it's primarily to get you to do things you should be doing anyway. But to benefit from compliance, you need to understand how it's structured, and how it fits into your SAP landscape and your business as a whole.

SAP Compliance Management & GRC

Compliance management refers to the controls put in place to restrict and monitor how users access, view and modify information within the SAP landscape. These tasks are handled by a Governance, Risk and Compliance program, such as ControlPanelGRC, or SAP GRC. These compliance management tasks include:

- Establishing an internal control structure
- Validating the effectiveness of internal controls
- Certifying the accuracy of financial statements
- Preventing tampering
- Reporting detailed financial information
- Disclosing confilicts of interest

GRC software monitors user access to identify potential segregation of duty and excessive access risks. For example, a single user shouldn't be able to complete multiple portions of a business transaction (e.g. creating and paying a vendor), change the record of a transaction, or modify a financial report so that it excludes or differs from information in the database. Monitoring excessive access is also a top priority; as critical business transactions should only be granted to appropriate individuals to prevent both fraud and errors.

GRC programs also need to monitor financial controls, and verify all access and changes to documents in order to create an audit trail. This supports authentication of important records; helps admins and auditors spot suspicious activity and bugs in the system; and provides a powerful disincentive against fraud, leaks and tampering. Finally, the GRC program needs to be able to organize and report on effectiveness of controls, according to compliance rules, while maintaining proper access control.

Auditors, investors and customers will all need access to different amounts of information, and much of the data auditors need could breach confidentiality or expose trade secrets if shared with other parties. Your compliance management program also needs to account for conflicts of interest and other mandated non-financial data.

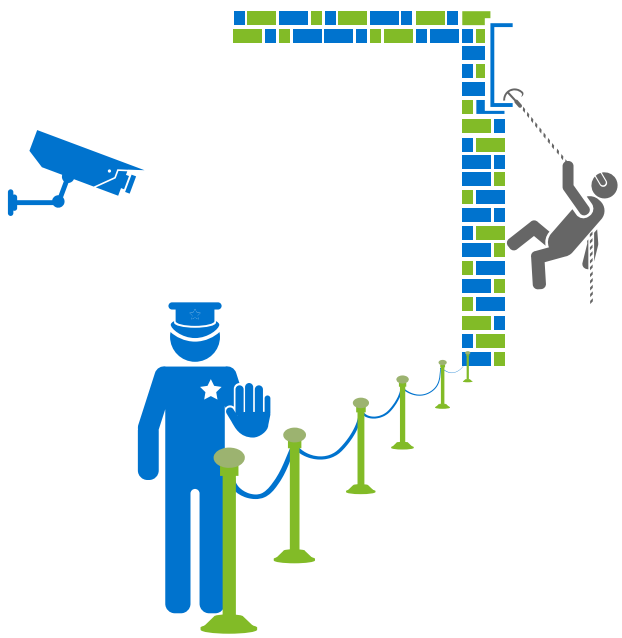
Compliance management is crucial to nearly everything your company does. It's how you verify payroll, sales or HR records, and protect information integrity and confidentiality. Whether it's a trade secret, a 21 CFR 11 medical study, or HIPAA PHI, compliance management plays a role in keeping it safe.

Cyber Security and Compliance

At the risk of oversimplifying it, GRC prevents people from misusing your system; while cyber security prevents them from breaking in. We can illustrate this by picturing security in a museum.

Standard (GRC) safeguards include:

- Guards to enfoce rules
- Ropes and cases to prevent theft of damage to assets
- Locked doors and alarms to restrict access to valuable assets
- Cameras and motion detectors for monitoring



But what stops thieves from picking a lock and cutting the power to dissable the alarm, or entering through a hatch in the roof? That's where cyber security comes in.

People get confused by the different things each compliance regime says about cyber security. For example, PCI requires specific technical safeguards like encryption across open networks, firewalls and the elimination of default passwords, while HIPAA emphasizes broader principles, training and legal frameworks like BAAs.

But under a security best practices approach, the differences are actually pretty minor. HIPAA may not technically mandate encryption or firewalls, but they vastly reduce HIPAA compliance risks. Similarly, PCI might not require BAAs, but it's in your company's best interest to make sure your partners are adhering to stringent data protection standards.

Process Documentation and Quality Management

It may sound obvious, but cyber security and compliance management initiatives won't go far, unless your company implements and consistently uses them — and that requires good process documentation. Everything from network configuration, to access control to daily system health checks and maintenance needs to be spelled out clearly and succinctly; the goal isn't impressive, weighty tomes — it's simple documents that spell out all necessary tasks.

This documentation needs to be incorporated into a quality management program. Although quality management doesn't focus exclusively on security and compliance, many aspects have important functions in this domain, including technology policies, SOPs, auditing procedures, training, document control, and audit trails. Putting it all together almost always requires outside help.

Choosing the Right SAP Security and Compliance Partner

A provider needs to understand the compliance requirements of your industry, but doesn't need to focus exclusively on them. Often, experience across multiple industries is a better sign of a company that understands security and compliance.

It's crucial, however, that your partner practices what is preaches. There should be a quality management program in place with things like:

Formalized Quality Policy, Quality Plan, and Procedures

- Audit trails
- Version control
- Sample installation qualifications

SOPs for critical systems should be recorded on controlled documents, approved by management, stored where no one can tamper with them, and trained and retrained regularly by anyone who does the work. Your partner should be ready to answer questions on anything from employee training and monitoring, to server hardening, to what happens when you call the help line.

In particular, they need good quality assurance, with separate task completion and verification staff. Finally, they should be ready to undergo regular 3rd party audits to assess and validate internal controls.

SYMMETRY

The Case for Bundling Security and Compliance with Managed Services

In the SAP hosting and managed services realm, companies that once had separate providers for hosting, IT project management, admin, DR/HA and so on, are moving to an integrated approach, citing benefits like lower cost, increased flexibility, greater knowledge base and less administrative overhead. In security and compliance management, however, tasks like IT security auditing, physical security auditing, GRC, monitoring and incident response are often farmed out to a web of different providers.

Forward-looking companies, however, are already starting to see the benefits of a unified managed services approach incorporating security and compliance. This approach lets you leverage your provider's internal controls and knowledge base, along with their auditing framework. The people auditing, monitoring and hardening your system can work directly with the people running it, meaning better communication, quicker results and a lower administrative overhead. In an emergency, you won't have to make frantic calls between your hosting provider, your database administrator and your network engineer — everyone is already working together, which means quicker resolutions, leading to better outcomes.

It also provides legal cover in the event of a breach, attack or outage. Successful hacks often simultaneously exploit weaknesses in hardware setup, software patching, GRC, training, monitoring and other domains. In a disaster, everyone goes into damage control mode, and you can end up with multiple agencies fighting it out in the courts (and in the press!) for years. If one provider handles everything, on the other hand, it's their reputation on the line.

Getting SAP Security and Compliance Management Right

The most secure organizations don't look at SAP compliance management and security requirements as roadblocks, but as a way to protect their investments. Governance, risk and compliance provides a powerful framework to protect your organization from errors, corruption and costly mistakes, and industry-specific compliance regimes provides similar fortification against external threats. Legal regimes and industry guidelines can't account for every threat an organization faces.

Partners like Symmetry view compliance regimes as more than just boxes to check, and as one aspect of an organization-wide program including risk assessment, training, auditing and monitoring.

Interested in learning more about SAP Security and Compliance? Contact your Symmetry representative or visit our website at:

www.SymmetryCorp.com
salesinfo@symmetrycorp.com
888-796-2677