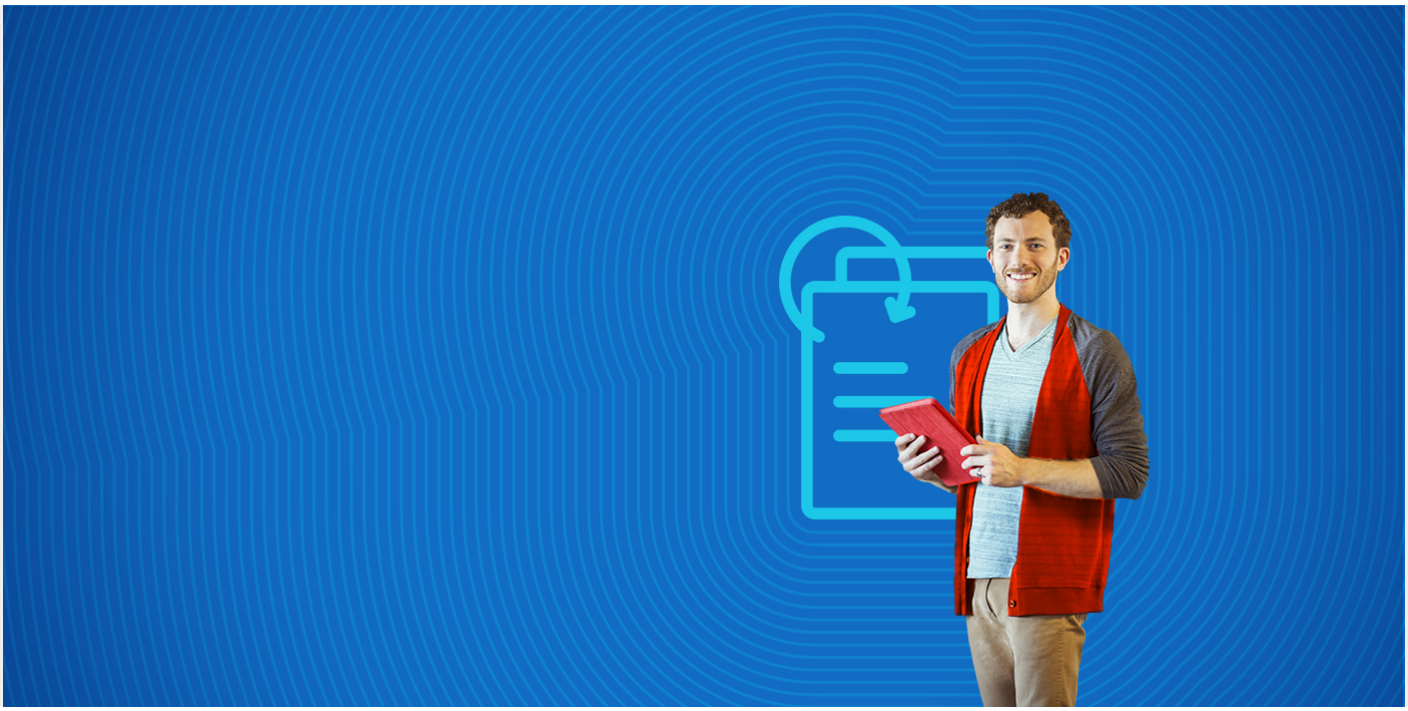
COMPLIANCE AUDITS: AN INTRODUCTION



Governance strategies for Security and Operations to reduce risk and ensure compliance

As the digital economy continues to explode and puts more pressure on enterprises for ensuring security and compliance, the challenges for meeting these requirements become even greater. With the growing amount of digital activity, it's more critical than ever to have a clear audit trail and action plan to address compliance requirements with automation that integrates best-practice processes to ensure security and compliance.

Compliance has been viewed in the past as mainly an administrative burden, however the world is changing. The risk of high-profile consequences from incomplete or insufficient attention to vulnerabilities or compliance failures continues to increase. Operations teams must maintain optimal configurations in their organization's infrastructure (including physical and cloud-based servers). At the same time, the Security team responsible for auditing and reporting on compliance with corporate or regulatory mandates needs to meet organizational and legal requirements. Both teams have to achieve these objectives, even with the increased pressure on budgets, fewer resources, and more frequent audits.

By taking a strategic approach to addressing security and compliance objectives, you can reduce the window of vulnerability, speed remediation, and reduce the time and effort required to keep an organization continuously compliant by managing by policy and not just by alerts. This strategic approach impacts IT configurations, including ongoing security scanning, regular compliance audits, and relevant processes such as change management.

Fast track security with TrueSight Vulnerability Management for Third-Party Applications

Explore TrueSight Vulnerability Management for Third-Party Applications ›
See how you can accelerate vulnerability resolution, lower costs of remediation and avoid major security incidents.

- Prioritize and remediate vulnerabilities with TrueSight Vulnerability Management for Third-Party Applications
- Reduce time spent logging changes in CM system
- Improve systems stability through granular, role-based access
- Explore the security view to see predictive SLAs and burndown with TrueSight Vulnerability Management for Third-Party Applications

What are the key compliance standards?

There are different types of audits that your organization may need to comply with based on your industry and geographic region. IT compliance typically relates to standards that may be internal or external. Examples of internal standards include operational or build standards requiring certain configurations, or the latest security patches. External compliance standards might include both best practices and security practice requirements imposed by industry or government bodies, such as Payment Card Industry Data Security Standard (PCI DSS) for retailers, Sarbanes Oxley (SOX) for publically traded companies, or Defense Information Systems Agency Security Technical Implementation Guide (DISA STIG) standard for U.S. federal contractors and agencies.

Some of the other additional external compliance standards include HIPAA (http://www.hhs.gov/hipaa/index.html), Center for Internet Security (CIS), DISA security policies, ISO standards, and FISMA.

What's enterprise governance?

Enterprise governance supports systematic business change by aligning security and technology investments and projects with business needs. It provides the overarching structure to ensure that the technology is delivered effectively to reduce risk, conduct audits, ensure compliance, protect assets, and continuously align security and technology with business needs.

- Risk management involves identifying, assessing and prioritizing risks. Resources are used to monitor, control and reduce risks. The risk management standards include ISO/IEC Guide 73:2009, ISO/DIS 31000, and NIST SP800-30.
- Audits pertain to evaluating, people, organizations, projects, processes, etc., to determine the validity and reliability of data and assess how a system is controlled internally.

What's the cost of failing to meet compliance requirements?

Organizations that cannot meet compliance requirements and fail to fully integrate the objectives of security operations teams spend too much time, energy, and money on reporting. More importantly, if they don't continually scan for security and compliance issues and automate the process of correcting them, they will eventually suffer security breaches and find themselves in a very difficult situation. Negative consequences of a breach may include:

- Direct costs related to communicating with affected users and customers, credit monitoring services, financial and even legal penalties.
- Indirect costs based on negative perception from media, organizational disruption due to investigation, possible reactive action not in line with strategic goals.

Both the possibility of a breach and its impact can be substantially reduced with a strategic approach to automation that brings the Security and Operations teams together to streamline communication for a better hand-off between these teams and a more effective outcome.

What are the challenges related to audits and remediation in the digital economy?

The demands of the digital economy drive so much high-speed activity with higher transaction levels and interactions that can open up an enterprise to more vulnerabilities. The complexity of the digital economy is exacerbated by an increase in cloud-based apps, virtualized data centers, and the growth of BYOD (bring your own device) to work.

There's often a lag between the time an audit is completed and the corrective action is taken because these efforts are done by two different teams with competing priorities. Historically, configuration compliance has been a two-step process. First, an audit compares the current state of IT systems to the appropriate policies, standards, and legal requirements on a regular basis. Second, the remediation process documents and corrects discrepancies between the desired configuration standard and the live configuration to bring the actual state in line with the desired state.

An audit report that lists security risks or discrepancies in configurations has some value, but it does not provide actual compliance. Today, this process is generally disconnected, with one team defining or adopting a certain standard and performing audits against that standard. However, the auditing team usually does not have access to correct any issues that have been identified, so they must send a list of those issues to the IT operations team for action.

Finally, it's easy to overlook something in an emergency, but when you plan ahead and include continuous automated discovery, you can achieve comprehensive coverage for your security and compliance efforts. Automated vigilant compliance makes both audit and remediation routine, ongoing activities – not emergencies.

How can automation ensure vigilant compliance and governance?

Vigilant compliance is based on managing by policy, and not just by an alert. It means that organizations need to assess their risks, streamline their processes, monitor security, and do closed-loop remediation. It's based on a holistic approach to governance that integrates and automates phases that include: discovery, definition, audit and remediation.

A governance policy is composed of these four areas and should leverage automation help to ensure vigilant compliance:

- **Discover:** Automated discovery delivers a complete picture of what is in the IT environment, as well as dependencies between different infrastructure components. The resulting inventory will be an up-to-date baseline with a complete list of systems that need to be audited for compliance, including any unofficial and temporary modifications to the known environment. It conducts a combination of active and passive, agentless discovery of systems on the network. Based on patterns of how individual systems communicate with each other, it maps out dependencies and business applications, which allow IT to prioritize effort (for instance, security response) based on the potential business impact of a breach or an outage.
- **Define:** Security teams can then define what the state of that environment should be, using patching information from vendors, third-party best practices, industry-specific policies, and particular requirements of each situation. Operations can leverage a number of pre-defined policies ready for use. Thanks to its detailed, actionable definition of the desired state, regular, scheduled, and automated audits are immediately available for action. Granular configuration visibility helps avoid false positives that would otherwise create an alert to a vulnerability that does not exist, as well as reduce false negatives that would otherwise miss a potentially harmful vulnerability.
- **Audit:** Security and Operations teams depend on tools and reports to conduct thorough audits without having to limit coverage due to the enormous effort of completing this step manually. Now, the team can audit on a regular basis to identify any departure from the desired state. They can compare live configurations to a reference system and troubleshoot issues caused by configuration discrepancies. Or they can evaluate the current state to a "known good" state from a prior period and use the snapshots to aid in troubleshooting.Another option is to compare the current state to out-of-the-box policies such as Sarbanes-Oxley (SOX) Section 404, Health Insurance Portability & Accountability Act (HIPAA), Payment Card Industry Digital Security Standard (PCI DSS) or Center for Internet Security (CIS), Defense Information Systems Agency (DISA), or they can use these standard policies as templates to build customized operational policies. It is easy to match patching levels to the latest recommendations from the vendor. Add in the invaluable data of vulnerability assessment tools, and the teams have actionable intelligence at their fingertips, including reports and logs.
- **Remediate:** The audit phase is designed to understand the difference between the desired and actual states. The remediation determines what action to take in response. Automated remediation is immediately available to address any identified issues and return the environment to the desired state in a timely and predictable manner. Remediation can be scheduled or triggered on demand, without the need of scripting. If an issue occurs, there is a built-in mechanism to easily roll-back to a prior "known good" state. Because of the high risk of errors when a change occurs, remediation can be used as a surgical tool, making only the changes that are required.
- **Govern:** Now it is possible to ensure control and visibility of all actions by keeping track of changes to the environment and why the change was made through the govern phase. For instance, there are many perfectly valid reasons for configurations to drift over time. Having those reasons properly documented ensures staff doesn't revert to an inappropriate state. In the same way, it may not be possible to deploy certain patches because of application compatibility issues.

By coordinating with the change management process, teams can enforce change windows and

avoid collisions or unplanned outages. Compliance may not necessarily require a configuration to be changed, and security requirements may be satisfied in other ways. But, it is important to document and track the exceptions. If exceptions to standard compliance practice are not organized and formalized in this way, the risk is that “almost compliant” becomes the new standard, since they can generate large numbers of false-positive alerts or worse, cause the organization to fail an audit.