BEST PRACTICES TO PASS AN IT SECURITY AUDIT

Reducing Risks and Costs for IT, Audit, and Security Teams

Table of Contents

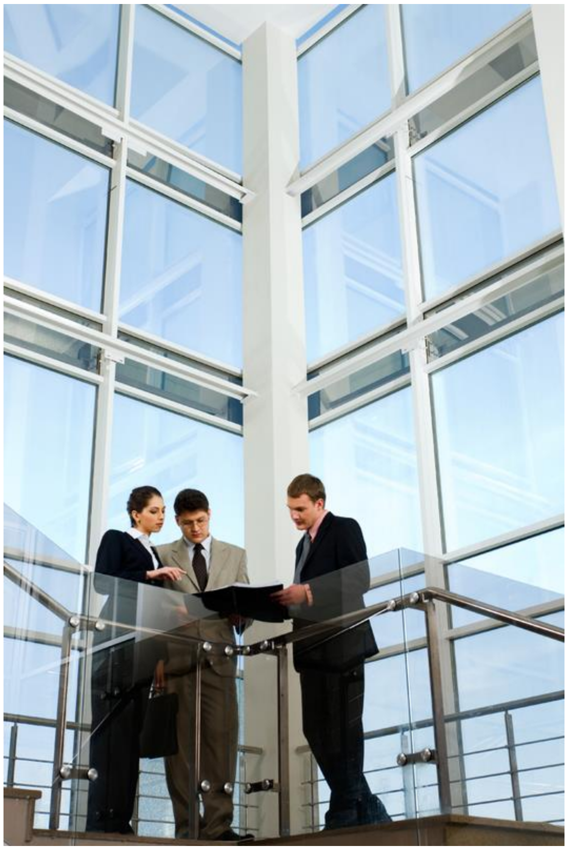
Most organizations are required to comply with several compliance regulations, including international and U.S State civil codes, which often mandate penalties for exposing intellectual property (IP) or Personally Identifiable Information (PII). Firms can risk fines, audit failures, lawsuits, and brand damage, with average costs now exceeding $4 million for litigation or security breaches, and $15 million or more for audit failures. Many firms also struggle to implement updates from the Center for Information Security (CIS), the National Institute of Standards and Technology (NIST), or the Cybersecurity and Infrastructure Security Agency (CISA). These frameworks often underscore Written Information Security Programs (WISPs), and failure to implement changes can lead to audit failures.

What follows is a detailed discussion of the internal and external regulatory challenges many organizations face, including the scope of these challenges and how they can be addressed through better business processes and automation. Solution recommendations can allow firms to improve security postures by reducing attack surfaces, complexities, costs, and risks.

"When I was lead security analyst at a large Fortune 500 financial institution, my firm was subject to many audits of our IT security. After trying several tools for Governance, Risk, and Compliance, we finally switched to Qualys Policy Compliance as a practical way to automate management of IT controls, verify compliance with policies, and document everything for auditors."

Josh Hankins, Chief Technical Security Officer, Qualys

I. Regulatory Challenges



Failing to comply with regulatory mandates and internal security policies is not an option for most organizations. In recent years, we've seen a dramatic increase in security incidents where firms have been decimated by cybercriminals. Shareholders, customers, partners, and employees have also paid heavy penalties. Information access is now ubiquitous, and sensitive PII and IP must be protected from exposure and exploitation.

To prevent negative impacts, protect the integrity of enterprise-stored information, and ensure customer privacy, new laws and regulations have been created or updated that govern almost all industries. Some of today's most well-known security requirements include:

SOX – The Sarbanes-Oxley Act of 2002 requires strict internal controls and independent auditing of financial information as a proactive defense against fraud—with potentially serious civil and criminal penalties for noncompliance.

HIPAA – The Health Information Portability and Accountability Act of 1996 requires tight controls over handling of and access to medical information to protect patient privacy.

GLB – The Gramm-Leach-Bliley Act of 1999 requires financial institutions to create, document and continuously audit security procedures to protect the nonpublic personal information of their clients, including precautions to prevent unauthorized electronic access.

NIST SP 800-53A Rev 5 – National Institute of Standards and Technology Special Publication 800-53 defines management, operational and technical security controls for the information systems used by U.S. federal agencies, including guidelines within 17 different control areas to protect the confidentiality, integrity and availability of systems and the information they host. Rev 5 adds 66 new base controls, 202 new control enhancements, and 131 new parameters to existing controls.

California Consumer Privacy Act (CCPA) – In June 2018, California passed AB 375, a consumer privacy act that could have more repercussions on U.S. companies than the European Union's General Data Protection Regulation (GDPR). CCPA takes a broader view compared to GDPR regarding private data, or PII. The challenge for security teams relates to locating and securing that data. The CCPA law allows any California consumer the right to see any of their PII a company might have, as well as a complete list of any third-party firms that were given that information. Also, CCPA allows consumers to sue companies if the privacy guidelines were violated, even if there is no breach. The cost of eDiscovery and litigation, even if an organization is innocent, can easily escalate into the millions.

PCI-DSS 4.0 – On March 31, 2022, the Payment Card Industry Security Standards Council published version 4.0 of its PCI Data Security Standard (PCI-DSS). The updated standards provide significant new guidance on the scope and applicability for requirements for small to medium businesses. PCI- DSS 4.0 now applies to any systems that could impact account data security, so any compliance solution agents must run on all your systems and operating systems. It allows for multiple "on-demand" assessments upon request, so you could be audited at any time and must be fully prepared. A new track, called a Customized Approach, requires valid documentation to prove controls, such as comprehensive reports against those controls.

GDPR – For European Union (EU) businesses that need to comply with the General Data Protection Regulation (GDPR), and U.S. firms that do business with EU citizens, there is now greater pressure to avoid an Availability Breach. This is essentially defined as a cyberattacker having unauthorized access to sensitive PI and PII, even if a full breach did not occur. Most organizations must report all security measures in place to address data breaches, prove they can ensure full compliance with all GDPR requirements, and validate that proper GDPR controls are in place and implemented correctly.

The above are only a few of the many federal, state, and international regulations that apply to specific industries and government agencies, and the regulatory environment is becoming far more complex in the years to come. In addition, enterprises typically maintain a large, evolving body of internal policies (WISPs) designed to protect the company's information resources, employees, customers, and brand reputation.

Recent Compliance Statistics

- On average, firms spend $5.5M on compliance versus $15M on non-compliance
- More than 60 percent of organizations suffered a security breach in 2021
- 41% of firms say compliance/policy tracking is a top five risk and compliance function
- The Institute of Internal Auditors (IIA) says 75%+ of audit teams lack adequate software
- According to Verizon's Data Breach Investigation Report, 40% of web applications were breached due to misconfigurations
- Vulnerability management is not enough to harden configurations

II. Compliance Objectives

Many organizations faced with multiple compliance requirements are now taking a more mature approach to this problem by adopting IT governance frameworks that can cover a large percentage of regulatory compliance mandates. Three of the most widely employed frameworks are:

COBIT 5 – The COBIT frameworks have become an industry standard for IT management and governance. COBIT initially stood for Control Objectives for Information and Related Technology, but with COBIT 5 the acronym was dropped. The changes between COBIT 4.1 and COBIT 5 include more emphasis on creating business value. The COBIT 5 framework, which was released in 2012, is based on five key principles: Meeting stakeholder needs, Covering the enterprise end-to-end, Applying a single integrated framework, Enabling a holistic approach, and Separating governance from management. COBIT 5 also combines the COBIT frameworks with others developed by ISACA, such as Val IT and Risk IT.

ISO 27001 – This is an international standard for the management of IT security that organizes controls into ten major sections, each covering a different topic or area. These are: business continuity planning, system development and maintenance, physical and environmental security, compliance, personnel security, security organization, computer operations and management, asset control, and security policy. ISO/IEC 27001:2022 replaces the previous international standard for information security management, ISO/ IEC 27001:2013. If your organization's existing ISO 27001 certificate expires prior to 2024, you must upgrade by re-certification.

An added benefit of adopting control frameworks is the creation of repeatable processes for compliance and security procedures. This has typically led to the ability to better cope with multiple regulatory compliance mandates and an overall reduction of compliance costs and efforts.

III. Accountability

Legitimate businesses have no option but to adopt policies and technologies to ensure compliance with relevant regulations and policies, and to document both the compliance measures and the results for audit purposes. In this increasingly complicated regulatory environment, the relationship between a company's IT department and the rest of the business is changing dramatically.

Failure to manage compliance with regulatory mandates and internal policies imposes serious legal and security risks to any company. Protecting customer data from loss, ensuring the integrity of financial data, and preventing leaks of intellectual property as well as private employee data have become top priorities. As top-level executives become more concerned about the stakes, they increasingly hold IT managers accountable for enforcing and documenting compliance with regard to electronic systems and networks. When it comes to evaluating the performance of the IT staff, compliance metrics and audit results are now as important as service level agreements (SLAs), system uptime, and performance statistics.

IV. Solutions

Misconfigurations and human error account for most security breaches, which can lead to data theft, lawsuits, brand damage, and audit failures. While 65 percent of senior executives cite compliance failure as a high-risk security concern, remediating compliance issues to reduce attack surfaces and avoid serious consequences remains a challenge.

Qualys Policy Compliance (PC) adds a critical layer to your enterprise defense-in-depth security stack to help prevent security breaches and audit failures that can lead to serious consequences. Qualys PC goes beyond vulnerability management by automating the labor-intensive process of assessing security configurations, settings, and controls with a single cloud solution, multiple sensors, robust policy library, and seamless integration. Offering the industry's most robust policy compliance solution, Qualys PC offers 850 pre-configured policies, 19,000 controls and custom scripts, 350 advanced technologies, and 100 regulations and frameworks to cover almost any mandate. Qualys has the only dedicated compliance team in the industry, including a dedicated QA team for six sigma accuracy. Also, a team of compliance researchers updating controls and regulations automatically.

Josh Hankins is the Chief Technical Security Officer at Qualys. As a security leader at a previous firm, he and his team implemented a goal to ensure their systems attained a "steady state" as quickly as possible to meet policy compliance requirements. Steady state refers to systems that are operating properly without major issues. Systems management is eased by automatic discovery and remediation of anomalies during normal timeframes. The computing environment will trend at about the 90 percent range for compliance. This may seem like wishful thinking to those who are using legacy Governance Risk and Compliance Management (GRCM) tools, but Hankins and his team achieved this goal by using Qualys PC.

"You should consider your ability, and that of your third- party providers, to withstand a cyberattack. You should take all appropriate steps to shore up your controls, including raising staff awareness: that may, for example, include re- running staff ethical phishing campaigns. Consider if your staffing levels are appropriate to deal with an elevated cyber risk."

UK Financial Conduct Authority, Russian invasion of Ukraine: operational and cyber resilience, March 2022

V. Implementation

Hankins and his team began the transition process to Qualys PC with the IT owners who were preparing for a new audit. The audit domain involved the UNIX team, and a previous compliance tool had provided them with a solid framework and a robust paper-based policy. Their strategy was to prioritize the transition by first addressing operating systems used on the majority of their servers, and then proceed to lesser-used UNIX-based systems. They used a seven-step approach to foster "buy-in" with the IT owners to facilitate a smoother and faster deployment of Qualys PC:

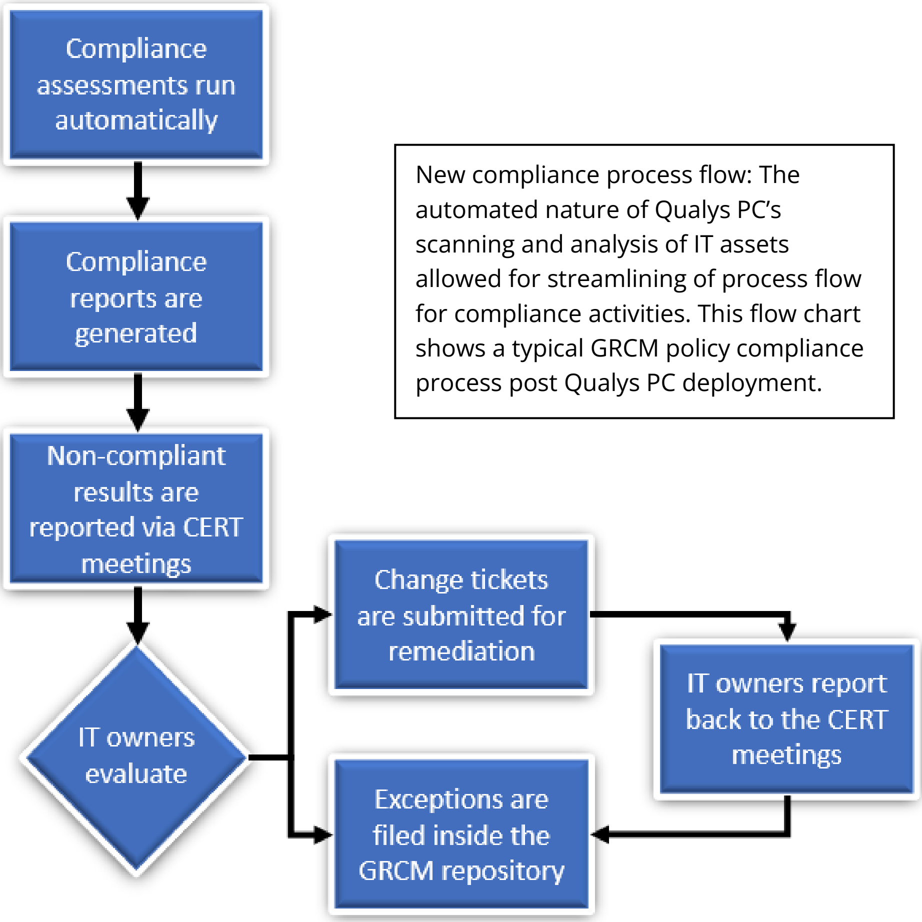
1. **A common goal –** An audit deadline loomed so there was no place to hide, and no time to waste.

2. **An incentive –** The last audit of UNIX systems did not go as planned, so there was a clear incentive to deploy a tool that would help them attain the highest rating. The audit could result in one of three outcomes: Satisfactory, Meets Requirements, or Unsatisfactory. Any rating less than Satisfactory shortened the break between audits, so they were motivated to do more than merely "pass."

3. **Ease of use and high value –** Qualys PC offered a significantly easier way to achieve better results, so IT owners were much happier using this to prepare for the audit. The Qualys Cloud Software-as-a-Service (SaaS) platform provided the team with more time to focus on the core goal of achieving "steady state" compliance. Efforts required to ensure agents were running before scanning were minimal and completed quickly. Saving time meant the team could focus on building controls and completing QA. The Qualys reports were accurate and easy to interpret.

4. **Audit surprise remediation –** Having previously dealt with numerous audit requests, the team found that some resulted in unwelcome "surprises." These caused considerable scrambling to get data to auditors quickly, such as emergency change tickets and creating ad hoc reports. The automated scanning and reporting provided by Qualys PC delivered a huge advantage for quickly creating accurate reports for auditors, and most especially for "audit surprises."

5. **New compliance process flow –** The automated nature of Qualys PC's scanning and analysis of IT assets allowed the team to streamline the process flow for compliance activities. The flow chart above shows the team's new GRCM policy compliance process.


Compliance assessments run automatically
Compliance reports are generated
Non-compliant results are reported via CERT meetings
IT owners evaluate
Change tickets are submitted for remediation
Exceptions are filed inside the GRCM repository
IT owners report back to the CERT meetings

New compliance process flow: The automated nature of Qualys PC's scanning and analysis of IT assets allowed for streamlining of process flow for compliance activities. This flow chart shows a typical GRCM policy compliance process post Qualys PC deployment.

6. **Leverage existing scanning data –** Qualys scanners were already distributed throughout strategic locations on the firm's network. This provided a turnkey solution for ramping up the new compliance solution faster and reaching the goal of a steady state for compliance.

7. **Proof of concept –** The UNIX team gained confidence with Qualys PC after they tested a sample cross section of systems that were representative of the production population. They performed targeted testing using test and QA systems, which proved that the new solution would not be detrimental to production systems.

8. **User defined controls –** Qualys PC provided the ability to fill in missing controls that were needed to complete the mapping of the paper policies in time for the next audit. The team did not need to wait on Qualys to create controls and could therefore finish the mapping process on time to ensure audit readiness.

VI. Results

For Hankins and his team, Qualys PC automatically scanned servers every week, which included more than 4,500 Windows and UNIX machines. The solution also created quarterly compliance reports for IT owners. These included "official" reports containing issues that IT owners needed to address throughout the next quarter. IT owners were required to show continuous remediation progress, and Qualys PC gave them the ability to login and see how systems were trending before publishing the next report. This empowered them to be proactive and enabled the security and compliance teams to stay ahead of the "audit curve." The Qualys PC reporting engine provided the flexibility to define reports with required details across four key policies:

- Windows Domain Controller servers for domain X
- Windows Domain Controller servers for domain Y
- Windows Member servers (non Domain Controller servers)
- Unix servers

Final report results

Auditors appreciated the level of detail in the compliance reports, specifically for the presence of control definitions and how each control was checked by Qualys PC. This information removed guesswork and enabled fast and automated delivery of accurate information to the auditors. The report template was mapped "one-to-one" to the paper policies. Josh Hankins and his team derived three clear benefits:

- Items were easy to read, follow, and more importantly to remediate
- Less confusion from an auditor's and IT owner's perspective
- Substantial time savings, as reports by previous tools were ambiguous and auditors would typically request a mapping of the controls in the paper policy to the controls listed in the tool. Essentially, Hankins and his team had the tedious chore of creating and maintaining a custom "compliance playbook" for every audit.

Hankins' Audit Preparation Checklist

- Have you identified all target assets? Check with your IT managers. They have a vested interest in helping you and themselves.
- Have you verified that all servers are scanned, and is there an authoritative source for all servers?
- Check with Configuration Management Database (CMDB) teams regarding business ratings
- Use the Qualys PC mapping tool.
- There should be a centralized IT Asset Database. If not, use the Qualys PC mapping tool and server subnets identified by the network team.
- Did the team remediate by severity? Consult IT owners to determine vulnerability priorities by prioritizing best practices such as NIST and CIS. Qualys PC can help with this.
- Are all feasible controls defined inside the reporting template based on current paper-based policies?
- Verify by examining the paper policies line by line. Your Qualys Technical Account Manager can help you ensure that paper controls are defined in Qualys PC.
- Is there evidence that IT owners have been actively remediating non-compliant issues?
- Save all documentation for auditors, including emails, meeting minutes, and Qualys PC reports.
- Are exceptions documented? Document your exceptions inside your GRCM repository tool. Track exceptions using Qualys PC.
- Are you prepared to address issues that are unresolved before the audit?
- Create a plan to address each issue. Describe each issue, what you will do for remediation, measurable milestones.
- Determine a closure date that is attainable by all teams involved.

VII. Conclusions

Josh Hankins has learned valuable lessons over the years regarding the administration of multiple IT GRCM tools. Having to do yet another migration is not desirable, but sometimes change is for the best. Using the industry's leading policy compliance solution can improve relationships with IT owners. This can lead to "buy-in" that controls are working properly and risks for security breaches, brand damage, audit failures, and litigation are greatly reduced. Hankins' and his team gained confidence that when reports were producing data, they were accurate and did not require additional wasted time to convince auditors that the data was correct.

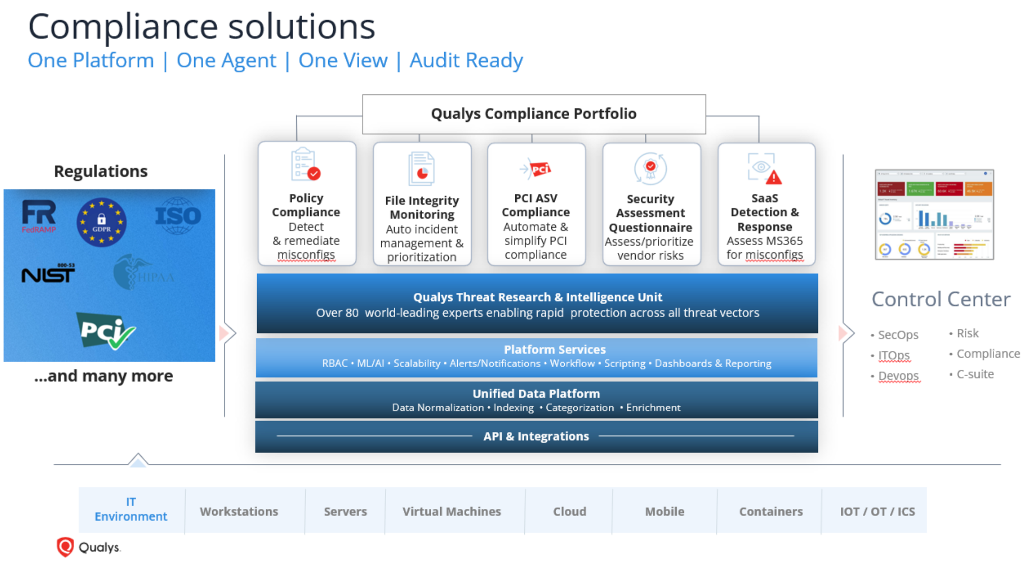
"Corporate culture and governance are not matters that you can 'set and forget'; they are enduring priorities for boards."

***ASIC's corporate governance priorities and the year ahead*, speech by Joe Longo, Chair at Australian Securities and Investments Commissions (ASIC), March 2022**

VIII. Qualys Compliance Leadership

More than 60 percent of organizations suffered a security breach in 2021 (Forrester). Misconfigurations and human error account for most breaches, which can lead to data theft, lawsuits, brand damage, and audit failures. Qualys customers have often avoided these serious consequences by adding Qualys Policy Compliance (PC) to their security stack alongside Qualys Vulnerability Management Detection and Response (VMDR).

The Qualys Compliance portfolio, which includes Policy Compliance and File Integrity Monitoring (FIM), enables organizations to have consolidated data gathered by Qualys sensors across all network segments, as well as simplified management and robust reporting from a single-pane-of-glass dashboard. Qualys PC and FIM go beyond vulnerability management to improve the ability to avoid security breaches and audit failures. Qualys approaches vulnerability and compliance management as a global issue that crosses your enterprise's organizational boundaries—and that encompasses an ever-growing and changing web of overlapping requirements.


Compliance solutions
One Platform | One Agent | One View | Audit Ready
Regulations
FR FedRAMP
GDPR
ISO
NIST 800-53
HIPAA
PCI
...and many more
Qualys Compliance Portfolio
Policy Compliance
Detect & remediate misconfigs
File Integrity Monitoring
Auto incident management & prioritization
PCI ASV Compliance
Automate & simplify PCI compliance
Security Assessment Questionnaire
Assess/prioritize vendor risks
SaaS Detection & Response
Assess MS365 for misconfigs
Qualys Threat Research & Intelligence Unit
Over 80 world-leading experts enabling rapid protection across all threat vectors
Platform Services
RBAC • ML/AI • Scalability • Alerts/Notifications • Workflow • Scripting • Dashboards & Reporting
Unified Data Platform
Data Normalization • Indexing • Categorization • Enrichment
API & Integrations
Control Center
• SecOps
• ITOps
• Devops
• Risk
• Compliance
• C-suite
IT Environment
Workstations
Servers
Virtual Machines
Cloud
Mobile
Containers
IOT / OT / ICS
Qualys