# HOW TO PASS AN IT AUDIT

## As told by an enterprise end-user who deployed QualysGuard Policy Compliance

**Table of Contents**



QUALYS®

As a lead security analyst at a large Fortune 500 financial institution, we're subject to many audits of our IT security. After trying several tools for Governance, Risk and Compliance, we recently switched to QualysGuard Policy Compliance as a practical way to automate management of IT controls, verify compliance with policy, and document everything for auditors. We were already a satisfied user of QualysGuard Vulnerability Management, so it made sense to leverage those automated asset and vulnerability scanning capabilities that are integrated with the QualysGuard platform.

We put QualysGuard PC straight to use on a pending audit of our UNIX environment, which hadn't done so well in the previous examination. Deployment was painless and our security team loved the easy to use capabilities that freed their time to focus on policy creation and testing. Most important: we passed the audit. The purpose of this document is to pass along tips we learned that may be useful as you consider adopting QualysGuard PC.

## Objective

My goal was to get our systems into a "steady state" as quickly as possible to meet requirements of our compliance policies. Steady state is when systems are humming right along without major glitches. Systems management is eased by automatic discovery and remediation of anomalies during normal timeframes. And the computing environment will trend at about the 90% range of compliance. This may seem like nirvana to some of you who are using legacy GRCM tools, but we have achieved this goal with QualysGuard PC.

## Migration Process

I began the transition process to QualysGuard PC with the IT owners who were preparing for a new audit. The audit domain involved the UNIX team. A previous compliance tool had provided us with a solid framework and a robust paper-based policy. Our strategy was to prioritize the transition by first addressing operating systems used on the majority of our servers, and then proceed to lesser-used UNIX-based systems.

## Audit Preperation Checklist

**Have you identified all target assets?**
Check with your IT mangers. They have a vested interest in helping you and themselves!

**Have you verified that all servers are scanned?**
Use the QualysGuard PC mapping tool.

**Is there an authoritative source of all servers?**
There should be a centralized IT Asset Database. If not, use the QualysGuard 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 weighing best practices such as NIST and CIS. QualysGuard PC can also help.

**Are all technically feasible controls defined inside the reporting template policy based on current paper-based policy?**
Verify by examining the paper policy line by line. Your Qualys Technical Account Manager can help you ensure that paper controls are defined in QualysGuard PC.

**Is there evidence that IT owners have been actively remediating non-compliant issues?**
Save all documentation for auditors, including emails with IT owners, meeting minutes, and QualysGuard PC reports.

**Are exceptions documented?**
Document your exceptions inside your GRCM repository tool. Track exceptions using QualysGuard PC.

**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, and closure date.

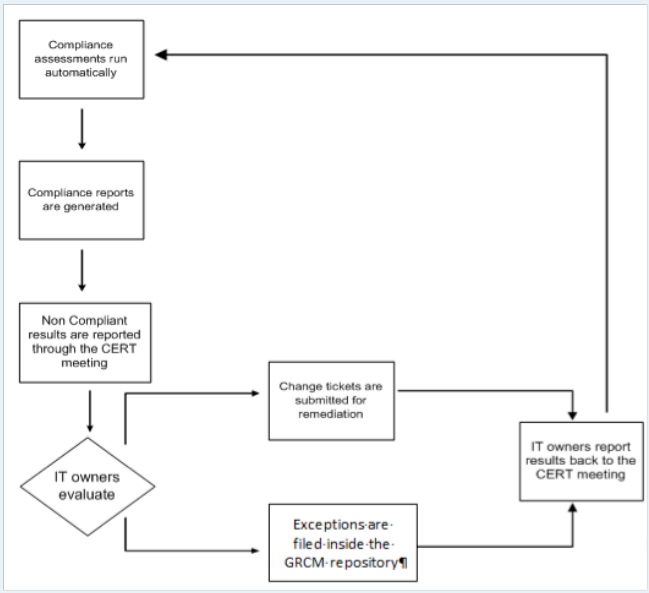
## Fostering Buy-in From IT Owners

I used a seven-step approach to foster "buy-in" with the IT owners to facilitate a smoother and faster deployment of QualysGuard PC.

1. **Rallied around a common goal** – An audit deadline loomed so there was no place to hide.

2. **Acknowledged the 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 us to attain the highest rating. The audit would result in one of three: Satisfactory, Meets Requirements, or Unsatisfactory. Any rating less than a satisfactory shortens the break between audits, so we were incented to do more than merely "pass" this audit.

3. **Emphasized ease of use and value** – QualysGuard PC offered a significantly easier way to achieve better results, so IT owners were much happier using it to prepare for the audit. The Qualys Software-as-a-Service (SaaS) system architecture provided the team with more time to focus our core goal of achieving "steady state" compliance. There were no agents to install and no cron jobs to code to ensure agents were running before scans. Saved time meant the team could focus on building and "QAing" controls. The Qualys reports were accurate and easy to interpret.




**New compliance process flow.** The automated nature of QualysGuard PC's scanning and analysis of IT assets allowed us to streamline our process flow for compliance activities. The flow chart shows our new GRCM policy compliance process.

4. **Swiftly dealt with audit surprises** – Over the past five years of my dealing with audit requests, some have resulted in unwelcome "surprises." These caused a lot of scrambling to get data to auditors quickly, such as emergency change tickets and creating ad hoc reports. The automated scanning and reporting by QualysGuard PC provided a huge advantage of delivering accurate reports to the auditors quickly, especially for "audit surprises."

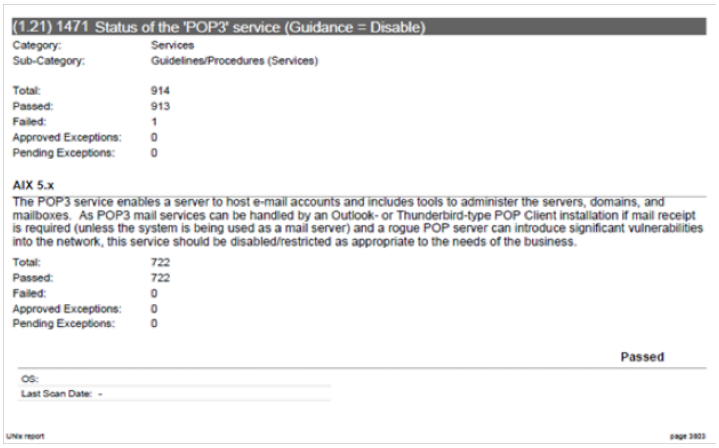
5. **Leveraged existing scanning data** – QualysGuard scanners were already distributed throughout strategic locations on the network. This was a big plus for it provided a turnkey solution for ramping up the new compliance solution faster and reaching my goal of a steady state for compliance.

6. **Used sampling for proof of concept** – The UNIX team gained confidence in QualysGuard PC after it tested a sample cross section of systems that were representative of their production population. Targeted testing was performed with test and QA systems proved that the new solution would not be detrimental to production systems.

7. **User defined controls** – QualysGuard PC provided us with the ability to fill in missing controls that were needed to complete the mapping of the paper policies in time for the next audit. We didn't have to wait on the vendor to create controls and thus we could finish the mapping process on time to be ready for the next audit.

## Results After We Deployed QualysGuard PC

QualysGuard PC automatically scans our servers every week, which includes more than 4,500 Windows & UNIX machines. It also produces quarterly compliance reports for IT owners. These are the "official" reports containing issues that the IT owners need to address throughout the next quarter. IT owners are required to show progress of remediation. QualysGuard PC gives the IT owners the ability to login and see how their systems are trending before publication of the next report. Getting an advance jump empowers the IT owners to be proactive and enables the security team and IT owners to stay ahead of the "audit curve." The reporting engine provided the flexibility to define reports with required details. We ended up with four policies:


(1.21) 1471 Status of the 'POP3' service (Guidance = Disable)

Category: Services
Sub-Category: Guidelines/Procedures (Services)

Total: 914
Passed: 913
Failed: 1
Approved Exceptions: 0
Pending Exceptions: 0

AIX 5.x

The POP3 service enables a server to host e-mail accounts and includes tools to administer the servers, domains, and mailboxes. As POP3 mail services can be handled by an Outlook- or Thunderbird-type POP Client installation if mail receipt is required (unless the system is being used as a mail server) and a rogue POP server can introduce significant vulnerabilities into the network, this service should be disabled/restricted as appropriate to the needs of the business.

Total: 722
Passed: 722
Failed: 0
Approved Exceptions: 0
Pending Exceptions: 0

Passed

OS:
Last Scan Date: -

UNIX report page 3803

**Example of a UNIX policy control in QualysGuard PC.**

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

### End results of the reports

Auditors appreciated the detail of the reports -- specifically, presence of control definitions and how each specific control was checked by QualysGuard PC. This information removed the "guessing" and we were able to deliver accurate information to the auditors quickly. The report template was mapped "one-to-one" to the paper policies. We saw three clear benefits: (1) items were easy to read, follow, and more importantly to remediate; (2) less confusion from an auditor's and IT owner's perspective; and (3) saved time. Reports by previous tools were ambiguous, so auditors would typically request a mapping of the controls in the paper policy to the controls listed in the tool. Essentially, we had the tedious chore of creating and maintaining a custom "compliance playbook" for every audit! That project sapped valuable time from the analyst's day and added yet more paperwork.

## Lessons Learned from My Experience with Compliance Tools

I have learned valuable lessons over the years of administering multiple IT GRCM tools. Nothing can make you rue change more than having to do yet another migration, but sometimes the change is good. Here is what I learned after deploying QualysGuard PC:

**A good compliance tool improves relationships with IT owners –** I developed a partnership with IT owners when "QAing" the controls. This led to their "buy-in" that the controls were working properly. Everyone gained confidence that when the reports are producing data, they will be accurate and won't require wasting time proving to auditors that the data is correct.

**Enforcing policy was easier with a good compliance tool –** QualysGuard PC helped us detect "configuration creep" of systems. IT management liked this feature because it ensured system administrators didn't stray from server configuration templates. The server configuration template was also evaluated by external and internal auditors.

**Remediation still requires good planning –** The automation and reporting provided by QualysGuard PC is a critical help to compliance, but you still need to coordinate action. I held recurring weekly meetings with IT owners and the vendor to go over "hot" items that needed immediate attention. By doing this, IT owners had a sense of ownership with this process. Our efforts focused on OSs that gave us the most "bang for your buck" (i.e. we started with the largest OS population) for developing a control set and applying remediation. Priority for remediation started with systems sharing these characteristics:

- Internet facing
- Regulatory implications (PCI, SOX, etc.)
- Internal prioritization (i.e. the Highs, Mediums, Lows).

**Allow adequate time for remediation –** Always allow enough "buffer time" for remediation to consider the number of systems effected, severity of the finding(s), resources available to remediate, and other compensating controls.

**Reprieves are usually possible –** If you offer up a remediation plan that seems reasonable and is measurable, you will typically get the timeframe you requested.

**SaaS is a winning architecture for compliance –** A big part of my success was due to the capabilities in the QualysGuard PC system architecture. The Software-as-a-Service (SaaS) design allowed us to focus our time on the more important items – composing policies, testing them, and reporting on the results. With SaaS, controls have the ability to become available quicker. I didn't have to download an update, apply a "hot fix" after testing it, or schedule a change ticket. Not having to rescan was a big plus, since the needed data points had already been harvested and retained by previous scans. The flexibility of implementing user defined controls to meet project/audit deadlines was also a key benefit. We didn't have to wait on the vendor to come up with the desired controls. We could build the items ourselves until the controls came out. The final reports presented were clean and easy to read. Compliance data was delivered on time and closed audits faster. Moreover, the cost of the new solution was 90 percent cheaper than the previous platform and it worked as promised, closing audits successfully and efficiently.

## Conclusion

Qualys Policy Compliance allows the analyst to be more productive by focusing time on analyzing the data and preparing for audits – instead of administrating the tool. Its capabilities allow organizations to stay ahead of the audit curve.

QUALYS®
www.qualys.com

**USA – Qualys, Inc.** • 1600 Bridge Parkway, Redwood Shores, CA 94065 • T: 1 (650) 801 6100 • sales@qualys.com
**UK – Qualys, Ltd.** • Beechwood House, 10 Windsor Road , Slough, Berkshire, SL1 2EJ • T: +44 (0) 1753 872100
**Germany – Qualys GmbH** • München Airport, Terminalstrasse Mitte 18, 85356 München • T: +49 (0) 89 97007 146
**France – Qualys Technologies** • Maison de la Défense, 7 Place de la Défense, 92400 Courbevoie • T: +33 (0) 1 41 97 35 70
**Japan – Qualys Japan K.K.** • Pacific Century Place 8F, 1-11-1 Marunouchi, Chiyoda-ku, 100-6208 Tokyo • T: +81 3 6860 8296
**United Arab Emirates – Qualys FZE** • PO Box 10559, Ras Al Khaimah, United Arab Emirates • T: +971 7 204 1225
**China – Qualys Hong Kong Ltd.** • Suite 1901, Tower B, TYG Center, C2 North Rd, East Third Ring Rd, Chaoyang District, Beijing • T: +86 10 84417495

ON DEMAND SECURITY