

Five Tips to Get IT Auditors Off Your Back

Written by Joe Grettenberger, CISA, CCEP Compliance Risk Advisor



Introduction

Establishing and maintaining a collaborative relationship with information technology (IT) auditors is the best way for organizations to improve compliance and reduce the stress of an audit. However, this type of relationship with auditors is not

always possible. This paper provides five proactive steps to take in planning for an audit. These steps can help you reduce the stress and distraction of an audit, while providing an even greater long-term benefit to your organization.

Five sources of IT audit stress

You feel the squeeze all around you. While keeping up with the demands of your users, you may have noticed that the sophistication of network attacks has been increasing. In the meantime, your network and systems vulnerabilities are multiplying, the organization is resizing, and you are working with a tighter budget, resulting in a smaller staff. Now you are faced with more legal and regulatory concerns, and, for some reason, your auditor has refused all of your requests for assistance in preparing for an upcoming IT audit that is scheduled during an already overloaded work week. What do you do?

Your level of stress both prior to and during an IT audit typically comes from five sources:

- Your knowledge of the current safeguards operating in your own environment
- Your knowledge of the potential areas of inquiry that are relevant to the audit (i.e., relevant risks)
- The actual state of your safeguards in light of the possible relevant areas of inquiry
- Your confidence in being able to quickly and adequately answer the auditor's questions
- The nature of your relationship with the auditor or audit group

As with any audit, your openness is critical to avoiding problems. However, when the practice of implementing safeguards with the help of an auditor's advice is not possible, to prepare for an audit you should focus first on improving your knowledge, then on your ability to respond, and then on the effectiveness of your internal controls. Here are five tips to help you accomplish these objectives.

Getting IT auditors off your back

When the practice of implementing IT safeguards in a collaborative relationship with IT auditors is not possible, focus on the following tips:

1. Adopt a proactive mindset to see the big picture
2. Familiarize yourself with what IT auditors want to see

3. Collect evidence using automation, and deliver reports daily
4. Avoid providing too much information
5. Use self-service capabilities when it makes sense

Tip 1: Adopt a proactive mindset to see the big picture

You and your auditor are ultimately working towards the same organizational goals. Your auditor is concerned with your organization's risk-taking activities and must verify that governing principles have been adopted in your area of operation. The auditor ensures that the controls (i.e. safeguards) you have in place are compliant with applicable laws while keeping risks within the limits that management considers acceptable.

When preparing for an audit of your IT systems, adopting a proactive mindset means:

- You have a plan to manage risks in the area under your stewardship
- The plan is approved by management
- You are following the plan
- You can demonstrate (via tools, documentation and reporting) you are following the plan and have been doing so consistently over a period of time

Tip 2: Familiarize yourself with what IT auditors want to see

As with all auditors, IT auditors try to ensure that the risks relevant to a particular audit concern are being appropriately addressed. This often means the auditor must verify that the controls within the audit's scope are being set up in a holistic fashion. For example, when reviewing the risks within an organization's user access controls, auditors of Windows-based systems will be interested in both the access control policies within Active Directory (AD), as well as the policies that control AD's administration.

With the automated configuration-checking technology that exists today, tools are available to report on candidate control weaknesses, as well as on suspicious activity these weaknesses may cause. Auditors evaluating system

To prepare for an audit you should focus first on improving your knowledge, then on your ability to respond, and then on the effectiveness of your internal controls.

and data access will likely want to see evidence of controls (such as system hardening) that protect against common vulnerabilities. In addition, they will want to ensure that appropriate data privacy settings are in place (such as access authorization), along with the traditional review of the organization's password policies. Auditors also want you to be able to account for all unauthorized access attempts (and login history) to systems containing protected information. In short, auditors want evidence demonstrating that appropriate controls are in place to prevent unauthorized access to your data.

Tip 3: Collect evidence using automation and deliver reports daily

The average cost of a data security breach is at an all-time high¹ while the level of sophistication of fraud and external cyber attacks steadily increases. If you are responsible for configuring your IT systems or the access permissions to those systems, the auditor will want to see what measures you've taken to reduce credible threats.

Preventative measures (which auditors call preventative controls) are a foundational component of virtually all audits. To establish evidence of effective preventative controls within your network, you must regularly check configuration and permission settings of your networked systems against acceptable limits, including operating system versions, applied patches, active system services, available system services, administrator access privileges, and other privileged user access. Reports on your findings that have been properly reviewed and approved are evidence of compliance.

If your organization is in an industry that lags behind others in adopting preventative controls, consider catching up by investing in appropriate technology and implementing up-to-

date countermeasure activities. Good information security and privacy controls will invariably include software that both enables and provides evidence of appropriate industry-current IT safeguards. These safeguards include automated controls such as: security baseline configuration checking; least privileged, role-based access; sensitive data tokenization; expanded use of encryption; true data loss prevention; well-tuned continuous monitoring, alerting and reporting; compliance evidence management and reporting; and dashboards that provide key metrics at a glance.

Regardless of the specific tools you choose, if you want to spend less time with your auditors, consider automating the process of collecting compliance evidence and delivering it daily to interested personnel. An even better idea would be to establish a policy that ensures appropriate personnel are reviewing and responding to the status of IT controls on a daily basis. That practice would be of keen interest to your auditor and, depending on your scope of responsibilities, may be enough to satisfy your auditor's interest in your area of stewardship.

Tip 4: Avoid providing too much information

Audits vary not only in type but also in degree. Normally, audits are conducted based on an audit plan. An audit plan contains the scope and priorities of the audit, based on all relevant risk areas. If the area under your stewardship is being audited, it is most likely because it falls within the scope and priorities of the audit plan.

Acquaint yourself with the audit scope to understand what risks are relevant to the audit you are facing. Depending on the type and scope of the audit and the identified risk areas, the auditor may require merely an interview or written

As with all auditors, IT auditors try to ensure that the risks relevant to a particular audit concern are being appropriately addressed. This often means the auditor must verify that the controls within the audit's scope are being set up in a holistic fashion.

¹Ponemon's "2009 Annual Study: U.S. Cost of a Data Breach" report, published January 2010, p. 14



If you want to spend less time with your auditors...establish a policy that ensures appropriate personnel are reviewing and responding to the status of IT controls on a daily basis.

answers to a few questions. If your auditor has not identified the area under your stewardship as a high-risk area, providing more information than what the audit team is requesting could invite unnecessary inquiry and potentially impede audit progress.

Tip 5: Use self-service capabilities when it makes sense

Self-service tools can often accommodate your internal auditors' requests by providing them with the query tools and reports most appropriate for their needs. For example, one way to spend less time answering audit-related questions is to consolidate your sources of compliance evidence into a near-real-time data repository with a standards-friendly reporting portal that supports ad hoc queries. However, you need to make sure it includes evidence of regular monitoring of approved configuration settings within your network, system, file, folder, user, and group configurations. Other ways to reduce time spent answering auditor questions might include providing predefined reports with intelligent filtering that reflect the health of approved IT safeguards operating within your environment or tracking key risk management and security metrics in a user-friendly dashboard with drill-down capabilities. Any of these tools can potentially reduce the time you spend with your auditors.

While not all areas of audit inquiry can be addressed this way, a significant portion can. The challenge is finding a solution extensive enough to address a significant portion of the audit scope applicable to your area of stewardship, and "feature-rich" enough to enable auditors to obtain compliance evidence in a timely manner. Such a solution could reduce your IT audit support hours considerably by enabling auditors to generate their own reports.

Conclusion

An IT audit shouldn't be stressful and disruptive, or difficult for your auditors. But it can be if you are not prepared. By understanding an IT audit's sources of stress and following the principles stated in the five tips described above, you can reduce angst as well as the time you need to spend with your auditors. Implementing these practices can increase your department's ability to quickly provide your auditors with the information they need, without interrupting your daily priorities, and ensure a faster, and potentially more successful, audit—even during the most arduous inspection. Moreover, applying these practices to the daily IT activities in your department can help further reduce long-term risk to your organization.

Appendix: Plan, secure and audit your Windows environment

The foundation of your internal control framework is your set of preventive controls: measures that reduce hazards and credible threats to data accuracy, security and privacy. Dell Reporter provides a wide range of reports that aggregate the status of system configurations and user account settings in Windows environments. When used as part of your monitoring activity, these reports can be presented as evidence of a preventative control framework and configuration status-checking activity within your organization's Windows infrastructure. And the specialty domain report packs in Dell Knowledge Portal are designed to deliver the appropriate evidence in a variety of common IT audit schemas.

Beyond delivering status reports of key preventative measures regularly to appropriate personnel and ensuring that the actions taken based on those reports are reviewed regularly by authorized personnel, the process itself should also be documented for the auditor. Such records can constitute substantive evidence of the relative health and maintenance of the preventative controls that exist within your IT infrastructure. Moreover, such evidence



is improved when the system of record demonstrates that configuration snapshots are regularly checked against your approved configuration baselines.

Dell Reporter can be used as part of a regular review and documentation process within the larger effort of maintaining proper preventative controls in the routine management of your network, system, file, folder, user, and group configurations. Such activities can provide evidence of infrastructure risk management that supports a variety of IT compliance efforts. Specifically, Reporter can be used to provide configuration snapshots in the following areas:

- System hardening
- Password policies
- Login history
- System configuration baseline checking
 - Hardware configurations
 - Operating system versions
 - Applied patches
 - Active system services
 - Available system services
- Least privileged, role-based access
 - Administrator access privileges
 - Other privileged user access and group permissions

Dell Reporter provides hundreds of predefined report templates with filtering and ad hoc query capabilities, plus configuration baseline checking. These reports support compliance evidence management and reporting in a variety of industry and regulatory formats. For more information on Dell Reporter, visit www.quest.com/reporter/. For more information about Quest Knowledge Portal, visit www.quest.com/quest-knowledge-portal/.

About the author

Joe Grettenberger has more than 22 years experience as an IT Assurance professional with 8 years of technology auditing experience both in the public and private sectors. Having started his own consulting practice in 2008, Grettenberger is certified as an information systems auditor (CISA) and compliance and ethics professional (CCEP). He currently serves clients as an IT governance and risk management consultant covering a wide range of IT assurance issues within the regulatory, legal, and industry compliance space.



© 2012 Dell, Inc. ALL RIGHTS RESERVED. This document contains proprietary information protected by copyright. No part of this document may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopying and recording for any purpose without the written permission of Dell, Inc. ("Dell").

Dell, Dell Software, the Dell Software logo and products—as identified in this document—are registered trademarks of Dell, Inc. in the U.S.A. and/or other countries. All other trademarks and registered trademarks are property of their respective owners.

The information in this document is provided in connection with Dell products. No license, express or implied, by estoppel or otherwise, to any intellectual property right is granted by this document or in connection with the sale of Dell products. EXCEPT AS SET FORTH IN DELL'S TERMS AND CONDITIONS AS SPECIFIED IN THE LICENSE AGREEMENT FOR THIS PRODUCT,

DELL ASSUMES NO LIABILITY WHATSOEVER AND DISCLAIMS ANY EXPRESS, IMPLIED OR STATUTORY WARRANTY RELATING TO ITS PRODUCTS INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTY OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, OR NON-INFRINGEMENT. IN NO EVENT SHALL DELL BE LIABLE FOR ANY DIRECT, INDIRECT, CONSEQUENTIAL, PUNITIVE, SPECIAL OR INCIDENTAL DAMAGES (INCLUDING, WITHOUT LIMITATION, DAMAGES FOR LOSS OF PROFITS, BUSINESS INTERRUPTION OR LOSS OF INFORMATION) ARISING OUT OF THE USE OR INABILITY TO USE THIS DOCUMENT, EVEN IF DELL HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. Dell makes no representations or warranties with respect to the accuracy or completeness of the contents of this document and reserves the right to make changes to specifications and product descriptions at any time without notice. Dell does not make any commitment to update the information contained in this document.

About Dell

Dell Inc. (NASDAQ: DELL) listens to customers and delivers worldwide innovative technology, business solutions and services they trust and value. For more information, visit www.dell.com.

If you have any questions regarding your potential use of this material, contact:

Dell Software

5 Polaris Way
Aliso Viejo, CA 92656
www.dell.com

Refer to our Web site for regional and international office information.

