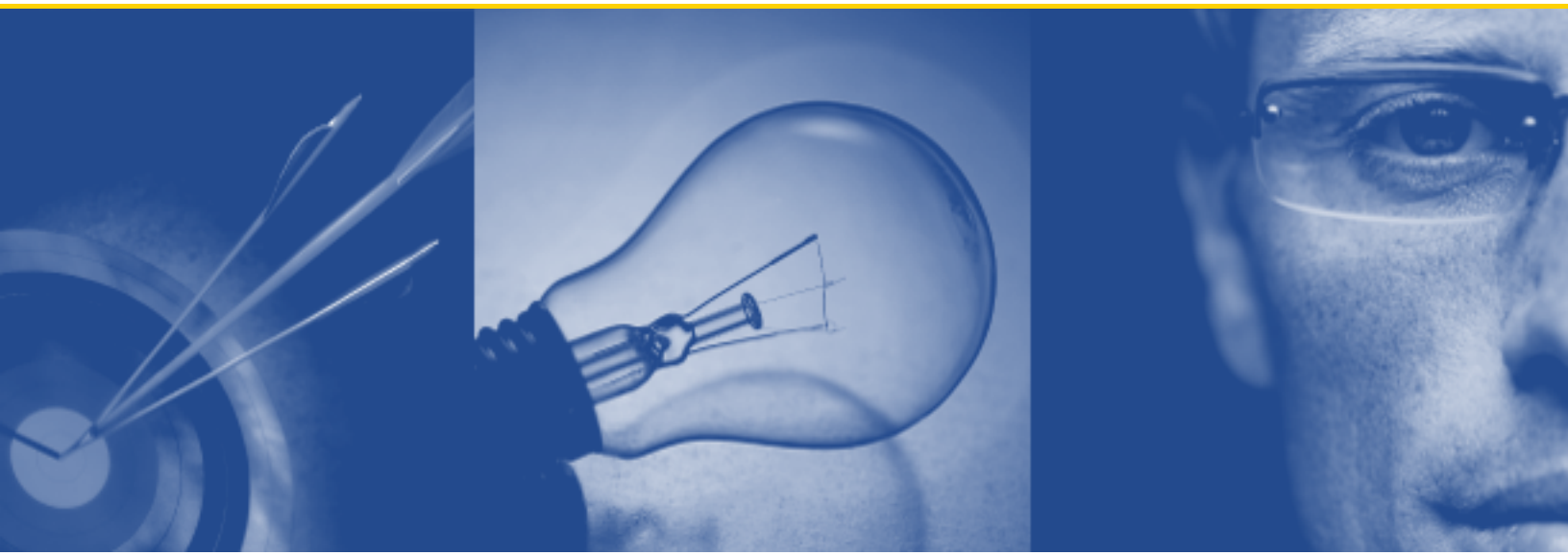
QUEST SOFTWARE®

# 10 Best Practices for Reducing the Stress of IT Audits

*Written by*
*Quest Software, Inc.*



## WARRANTY

The information contained in this document is subject to change without notice. Quest Software makes no warranty of any kind with respect to this information. QUEST SOFTWARE SPECIFICALLY DISCLAIMS THE IMPLIED WARRANTY OF THE MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. Quest Software shall not be liable for any direct, indirect, incidental, consequential, or other damage alleged in connection with the furnishing or use of this information.

## TRADEMARKS

All trademarks and registered trademarks used in this guide are property of their respective owners.

World Headquarters
5 Polaris Way
Aliso Viejo, CA 92656
www.quest.com
e-mail: info@quest.com
U.S. and Canada: 949.754.8000

Please refer to our Web site for regional and international office information.

Updated—August 13, 2008

# CONTENTS


INTRODUCTION ..... 1

DEFINING OUR TERMS ..... 2

THE CONTROL STACK ..... 3

10 TIPS FOR REDUCING THE STRESS OF IT AUDITS ..... 6

1. IF POSSIBLE, COLLABORATE WITH INTERNAL AUDITS ..... 7
2. IDENTIFY AND MANAGE YOUR SENSITIVE DATA ..... 9
3. PROTECT COMPONENTS SUPPORTING CRITICAL BUSINESS PROCESSES FROM COMMON THREATS ..... 10
4. SUPPORT YOUR LOCAL CHANGE MANAGEMENT PROCESS ..... 10
5. AUTOMATE WHERE IT MAKES SENSE ..... 11
6. KNOW THE LIMITS OF YOUR RESPONSIBILITY ..... 12
7. KNOW WHICH CRITICAL BUSINESS PROCESSES YOU ARE SUPPORTING ..... 12
8. GET YOUR HOUSE IN ORDER ..... 13
9. FOCUS ON FOUNDATIONAL CONTROLS ..... 14
10. ALIGN YOUR CONTROLS WITH YOUR BUSINESS STRATEGY AND GOALS ..... 14

CONCLUSION ..... 16

APPENDIX A ..... 17

QUEST SOFTWARE AND THE TOP 10 PROCESSES YOUR IT AUDITOR WILL WANT TO SEE ..... 17

APPENDIX B ..... 21

SAMPLE SCHEDULED REPORT LIST ..... 21

ABOUT QUEST SOFTWARE, INC. ..... 25

CONTACTING QUEST SOFTWARE ..... 25
CONTACTING QUEST SUPPORT ..... 25

# INTRODUCTION

Stress-free IT audits? Impossible, you say? An oxymoron? Well, consider this: there are proven ways to limit the time, effort, and cost impact of preparing for and undergoing IT audits, especially recurring audits, without taking your company private. While IT audits performed by external auditors are typically not trivial, there are significant ways to reduce the stress they induce. And for internal audits, organizations have even more options. This paper presents 10 best practices that can greatly reduce or even eliminate the angst so commonly associated with IT audits.[1]

[1] The information presented herein is made available solely for general informational purposes for companies facing regulatory compliance initiatives that include an IT component. While every effort has been made to confirm the accuracy of the information, the information provided may not be complete or accurate, may not be applicable to you and may not reflect recent developments in your regulatory environment. You should not act or refrain from acting based on the any of the information provided by Quest without first obtaining guidance and input from your professional advisors, including qualified counsel. This information is provided "as-is" and Quest disclaims all representations and warranties, express or implied, statutory or otherwise, including the implied warranties of merchantability and fitness for a particular purpose.

# DEFINING OUR TERMS

When you are discussing the compliance of areas under your supervision with an IT auditor, there are a few terms that are helpful to know. In fact, if you don't know these terms, reasoning with an auditor may be difficult.

## Controls

In laymen's terms, a control is a safeguard or countermeasure that organizations have in place to help ensure they achieve their primary business objectives. Most organizational controls are *internal controls*. These are manual, semi-automated or automated policies, procedures, processes, organizational structures, system settings, or program logic designed to keep risks that threaten business functions within acceptable limits. This ensures that the objectives of the enterprise are met (such as accurately stating the financials of the organization).

But every control should also have a more specific purpose that is well understood by management. To help management understand a control's particular purpose, each control should correspond to one or more secondary objectives, which auditors call *control objectives.*[2]

Because IT audits are often integrated with a larger audit of an organization's regulated practices[3] they are often performed within a control assessment. These typically begin in a top-down fashion with a review of business level assertions that correspond with an organization's entity-level controls (see Figure 1).

[2] Many standards, frameworks, and models are available to help organizations develop their own baseline of these safeguarding-type business objectives. Such a baseline may already be in use within your organization. Depending on the type of IT audit you are facing, a minimum set of controls (or control objectives) may be required and constitute the success criteria of the audit. Control objectives are ideally (and in some cases are required to be) reviewed and approved by the organization's senior management. If your organization has not identified and implemented a baseline of controls, or if there is one but it does not apply to the IT environment, your IT auditors will be compelled to perform their audit using a prescribed IT security standard or an IT control framework of their own.

[3] Examples include 1) publicly submitted financial statements, 2) storing personally identifiable information that is protected by law, 3) storing credit card data, and 4) making claims related to the security of an organization's services.

# THE CONTROL STACK

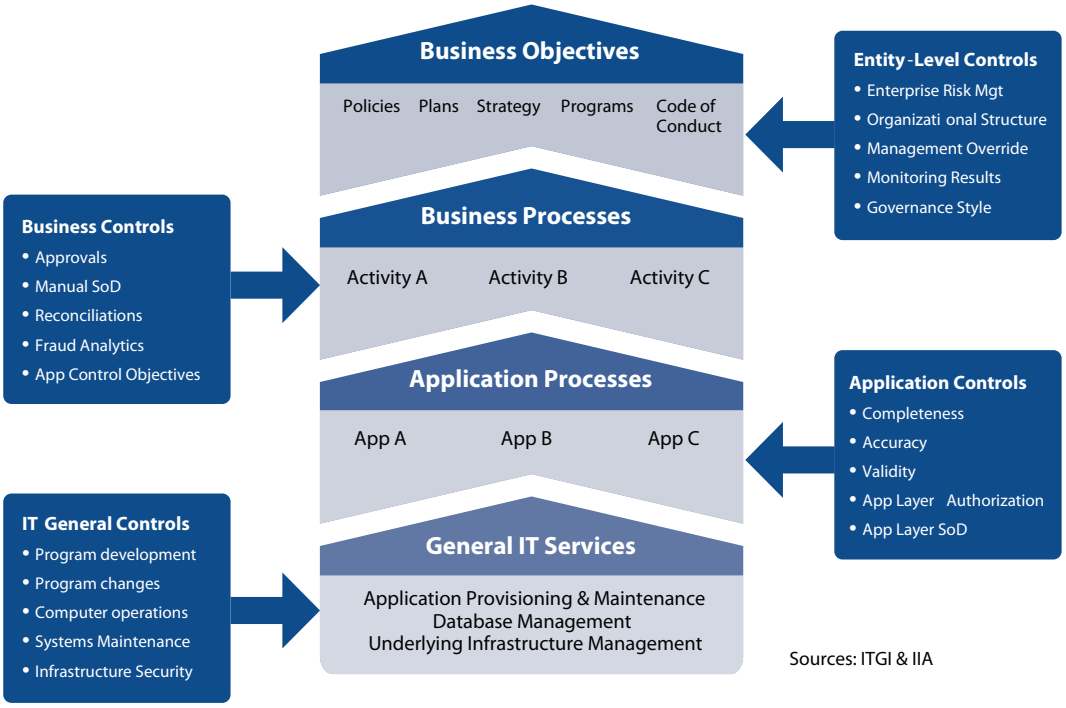



**Figure 1: The control stack**

However, the substantive control testing of an IT audit usually does not begin until the control assessment has reached the level of IT general controls.[4]

# IT General Controls and Application Controls

IT general controls (ITGCs) are the controls that are embedded in the systems that make up the IT infrastructure and assigned to the people providing IT services. ITGCs support business functions to the extent that the organization's business processes rely on technology. ITGCs are often contrasted with *application controls,* which are managed by business process owners.[5]

[4] This statement assumes that application controls are tested as part of the "larger audit." However, sometimes application controls are regarded as part of IT audits.

[5] Historically, ITGCs relate to computerized functions in an organization's IT infrastructure below the business-managed application layer of the technology stack. However, this perception is in flux somewhat as ownership and the need for control of the business application layer continues to sort itself out (e.g., e-mail content, collaboration software, spam filtering, mobile device content, personal storage devices, and other technologies that enable end-user managed content).

## Control Objectives

Organizations basically have three categories of expectations for their information systems. They expect them 1) to come with useful features and functions, 2) to be available for use when needed, and 3) to be protected from tampering.

Sometimes one or more of these expectations is passed off as being "patently obvious" and therefore "direction enough" for the IT department. Yet, as elemental as these goals may sound, they have proven insufficient in guiding those who design and maintain information systems. In the end, IT departments simply need those pesky details that explain "how," "in what way," and "to what degree" or they will fail at their job. For these and a variety of other reasons, expectations for an information system need to be made explicit.[6]

Even when not explicitly stated, control objectives are implied with virtually every new request of functionality that comes from the user community. Not convinced? Consider that companies not only expect their IS department to offer new capabilities to keep current with advances in technology, such as receiving e-mail via PDAs, (i.e., meet *capability objectives*) and to make these capabilities available at least during business hours (i.e., meet *service level objectives*). They also expect the technology to be sufficiently tamper resistant (i.e., meet *control objectives*). When proper controls are not in place, it's only a matter of time before someone complains.[7]

[6] To establish absolute minimums, expectations for information systems are sometimes (but not always) formulated into "requirements." For example, when funding for a new project is approved, business segments within an organization will often be required to specify information system *requirements* so that the capabilities (i.e., features and functions) desired by the business can be reviewed for the optimal method of fulfillment (i.e., assigned to procurement, assigned to an architecture team within the organization's IS department, or outsourced and become terms in a service provider agreement). A somewhat less binding term that can be used for setting an expectation is "objective"; objectives state desired outcomes without the precision that requirements demand.

[7] For example, the need for a control objective is abundantly clear when someone discovers that an employee in the shipping department was able to log into the payroll database and see the earnings of his team members. In such a case a control objective that was implied (but apparently not sufficiently communicated) is now made explicit ("enable business area owners to restrict access to protected data for all system users who do not have a need to know").

## Risks, Materiality, and Control Effectiveness

When performing an audit, auditors have a responsibility to look at the various types of risk being assumed (intentionally and unintentionally) by the organization. They will then weigh those risks on a scale that indicates risk significance. Astute auditors will consider the organization's entire control stack and look at the risks of undesirable incidents holistically. Undesirable incidents include theft, fraud, data leakage, security exploits, security breaches, sabotage, unauthorized change, unauthorized access, other significant policy violations, system failures, anomalies, and outages.

To merit the attention of an auditor, a risk must meet both of the following criteria:

- The risk has a reasonable possibility of occurring (or recurring).
- The risk would have a significant or material[8] impact on the company or its shareholders if realized.

Risks that do not meet both of these criteria do not merit the attention of the auditor (unless evidence of something particularly disturbing, such as an illegal act, exists[9]). Once potentially reoccurring risks are identified, they should be classified by management as significant, material, or neither. Then they should be prioritized and proactively addressed with carefully selected control objectives (see tip #7 in this paper for more information about this process).

*Control effectiveness* is defined as the amount that implemented controls mitigate material risks within the organization and meet the control objectives approved by management.

---

[8] It should be sufficient for our purposes to use the definitions provided in the auditing standard associated with Sarbanes-Oxley as an example of the distinction commonly made between material and significant risks. The Public Company Accounting Oversight Board's Auditing Standard No. 5 provides the following helpful definitions.

- Significant deficiency: "a deficiency, or a combination of deficiencies, in internal control over financial reporting that is less severe than a material weakness yet important enough to merit attention by those responsible for oversight of the company's financial reporting."
- Material weakness: "a deficiency, or a combination of deficiencies, in internal control over financial reporting, such that there is a reasonable possibility that a material misstatement of the company's annual or interim financial statements will not be prevented or detected on a timely basis."

[9] Any evidence of unlawful activity is an exception to the rule that risks need to meet both criteria to merit the attention of the auditor. Even a single illegal act that is discovered during the course of an audit obviously merits the attention of the auditor.

# 10 TIPS FOR REDUCING THE STRESS OF IT AUDITS

Do you worry about your next IT audit? Here are 10 tips that can reduce the stress induced by IT audits. Some tips apply to specific areas of responsibility (such as IT staff or IT managers); therefore not all tips may be applicable to your role, your department's style, or your organization's culture. But regardless of your role or your organization, you are sure to find something here that you can use.

## The 10 Tips:

1. If possible, collaborate with internal audits.
2. Identify and manage your sensitive data.
3. Protect components supporting critical business processes from common threats.
4. Support your local change management process.
5. Automate where it makes sense.
6. Know the limits of your responsibility.
7. Know which critical business processes you are supporting.
8. Get your house in order.
9. Focus on foundational controls.
10. Align your controls with your business strategy and goals.

# 1. If possible, collaborate with internal audits

Your internal audit department can potentially add value to the process of prioritizing your risks. If culture permits and no conflicts of interest are present, consider partnering with them to review the areas of risk related to the systems under your control. When possible, work with them to arrive at an agreement on the set of controls that you need to manage. (If you know for certain that this would never work with your internal audit department, you can skip the next subsection).

## Collaborating with Internal Auditors

In place of the traditional fear-based relationship with auditors, try to develop a working relationship with them built on trust. You could even be proactive about audits by reaching out to your internal auditors before they come your way. Let them know you want to help them. This may sound counterintuitive, but such actions can go a long way towards preempting potential snags that could arise from an audit you will eventually need to face.

For example, you can ask your internal auditors if there are any especially critical events from your event logs that you can help them track. The reports from these event logs can provide your auditors with enough evidence to support infrastructure controls for a continuous audit approach. See Appendix A for a sample scheduled report plan. As you review it, you may decide the reports are worth running for your own benefit. And as a best practice, you can implement an auditor-friendly continuous monitoring program based on the reports. Offering to share this information with your internal audit department provides the following benefits:

- Helps develop a non-adversarial relationship with internal auditors
- Leverages your internal audit function to support external audits
- Supports auditors in their role of providing visibility to management
- Enables auditors to build a continuous audit approach (if they feel so inclined) to auditing the systems under your responsibility that can eventually make all future audits of your environment stress-free.

Another possible point of collaboration is to ask your internal audit department to provide your group with guidance in conducting a self-assessment that includes a gap analysis and a remediation plan. Ask for specifics of what they will be looking for when they audit (or at least the general territory) so your self-assessment will be accurate. You can get on the good side of the auditor mainly by showing an interest in making their lives easier and helping them find what they are looking for faster.

## When Collaborating with Internal Auditors isn't Possible

Now for the reality check. If your internal audit group is resistant to all such collaboration, there are still steps you can take. While it is certainly easier when the relationship between internal audit and IT security staff is not adversarial, an agreement must be reached between these groups about which controls are expected to be operating within the organization's IT systems. Both groups must resist selecting controls that run contrary to management style or hinder business objectives unless the controls are required by mandate. Thus, a governance function that takes both business objectives and management style into consideration should be incorporated into the process of selecting the controls an organization adopts for its control baseline.

Below are a few steps you can take when your internal audit department is unavailable to assist you in the process of identifying material risks within your environment.

1. Ask the internal audit department for the company's official list of critical business processes deemed "key" for audit purposes.
   (They should at least give you that.)
2. Begin the process of identifying the systems, the protected data, and methods of protected data access under your supervision that support "key" business processes (see tip #7).
3. Focus your pro-active audit preparation efforts on improving controls for those systems (see tip #8).
4. Appeal to auditors on the basis of risk and materiality.

Whether by consensus, through a collaborative effort, by persuasion from IT security personnel, by management fiat, or by simply taking the internal audit department's word for it, it is vital to get agreement with internal audit on exactly which controls IT's operational configuration items (the data, systems, identities, roles, accounts, groups, and privileges) will have and how control effectiveness will be assessed.

For extra credit, you can:

1. Familiarize yourself with the company's approved baseline of internal controls (adopted and adapted control framework).
2. Familiarize yourself with the internal audit department's framework for assessing internal controls.

# 2. Identify and manage your sensitive data

Virtually all of the technology-related compliance mandates that companies face today require putting controls around certain types of sensitive data (phi, PII, cardholder data, sensitive financial data, etc.). Yet reactive one-off controls still prevail as the most common way of meeting these requirements. With the proliferation of compliance mandates, it makes sense to eliminate the implementation of stop-gap data security measures for each new mandate and move to a harmonized approach.

Even if the limits of your responsibility include only a few servers that store sensitive information, it's both effective and efficient to know:

- Which data types you have
- Where the data are stored
- What paths the data travel on
- What your data retention requirements are

Begin by making yourself aware of the data types your company deems sensitive (your internal audit department can identify the relevant sensitive data categories for your organization) and any special sensitive data requirements or restrictions (data encryption, hashing, masking, footprint reduction, life span tracking, removal, etc.). If you are in management and feel unsure about the scope of the sensitive data managed by your company, you can work at the organizational level to get a general sense of the data's overall "footprint" (leveraging appropriate data discovery tools where it makes sense). The goal is to move towards a proactive data management program ensuring sensitive data is:

- Addressed with specific policies
- Protected from unauthorized access (i.e. with specific groups and roles)
- Tracked when copied (to e-mail, spreadsheets, etc)
- Monitored for access (including temporary access)
- Monitored for change (including emergency changes)
- Promptly deleted when no longer required (by law, by contractual obligation, by litigation hold, or by your data retention policy).

# 3. Protect components supporting critical business processes from common threats

Certain processes are absolutely essential to making your business successful. This means the business applications that support those processes are critical. In addition to ensuring that adequate controls exist to manage protected data, it's important to know which infrastructure components support the business applications deemed critical to running your business.

Make sure your critical infrastructure components (databases, servers, and network devices) are identified and appropriately managed. In particular, make sure they adhere to minimum security configuration baselines (such as those offered by the Center for Internet Security) and that they are continuously patched for the latest security vulnerabilities.

# 4. Support your local change management process

If I had to pick only one process to focus on for improving IT operations, I would pick change management. Ensuring that changes to critical items under your control go through a concerted change management process is critical to preparing for IT audits.

Listed below are the top ten risk indicators of poor or non-existent change management. Any one of the following discoveries in an IT control environment would be an alert to the potential of poor change management.

- Unauthorized changes
- Unplanned changes
- Low change success rate
- High number of emergency changes (in excess of 15%)
- Delayed project implementations
- Untested or inadequately tested changes
- No test environment for testing changes, or an inadequate test environment
- Situations in which the affected business owner is not part of the review and testing process
- Inability to roll back or restore production to a known state
- IT operating in continuous firefighting mode

# 5. Automate where it makes sense

As explained above, controls provide assurance of business process integrity. Thus, control automation is the embedded assurance portion of automating business processes and ITGCs. Controls can often be automated or partially automated with software. For example, software with a notification workflow feature that supports approval matrices can be used to automate a manual approval process (such as requests for elevated privileges).

Control automation also makes business processes more efficient and less vulnerable to human error. But automating all IT controls is not practical: effective control automation requires prioritizing your manual processes. Good candidates for automation include the following:

- Manual controls that are the most error prone.
- Processes that will save significant time, cost, and effort.
  Examples include:
    - Approvals
    - Continuous monitoring
    - Intelligent audit trails

Specifically, continuous monitoring can greatly benefit internal auditors, as explained in tip #1. If you can automate monitoring and help implement computer-assisted auditing techniques (CAATs), you are a big winner.

Control automation can greatly reduce costs of sustaining compliance over time because the initial effort is a one-time cost. Automating internal controls tends to demystify the external auditor's control testing process and shorten the audit engagement. It's hard to justify billing hundreds of hours for "testing" key internal controls if control automation pervades the enterprise.

To summarize, the efficiency provided by control automation offers businesses at least three ways to save money:

1. Reduced cost of maintaining internal controls
2. Reduced outside auditor hours
3. Fewer internal resource hours spent supporting compliance audits

# 6. Know the limits of your responsibility

Businesses that experience damaging consequences of corporate malfeasance or improper data changes often think only IT needs to be changed. But, as we have seen, controls can (and should) be applied in many other areas of a company.

For example, at the application layer, IT's role is actually quite limited. IT can and should oversee the change management process to curtail unauthorized changes to computer systems (i.e., control changes to ITGCs), but changes that affect data integrity within an organization's business applications (as well as changes to business application settings or application layer user roles and privileges) are better managed by business process owners. Businesses must look beyond IT in order to enforce corporate policy and change employee behavior.

# 7. Know which critical business processes you are supporting

Understanding both the business objectives and business processes your systems support are the most important steps you can take in managing risk within your sphere of responsibility. Identifying those critical business processes that rely on your systems and data will not only help you determine nature and extent of the controls you need (or don't need) in your environment; it will form the foundation of the risk model for managing your risks.

However, the risks need to be quantified and approved by management to be defensible. This practice is the key to prioritizing which risks you need to manage. It serves as the basis of negotiating with auditors about what is and is not "material" in an audit. If you have done your job here correctly, you can stand your ground in justifying what's in scope and what's not in scope for risk-based audits like SOX and other ICFR audits.

Want more details? Below is the outline to an approach from the Institute of Internal Auditors (IIA) that is publicly available from their web site for identifying and assessing IT risks.[10] It can be used by both auditors and non-auditors alike.

### GAIT-R Top-Down Methodology

1. Identify the business objectives for which the controls are to be assessed.
2. Identify the key controls within business processes required to provide reasonable assurance that the business objectives will be achieved.
3. Identify the critical IT functionality relied upon, from among the key business controls.

[10] GAIT for Business and IT Risk, The Institute for Internal Auditors, March 2008.

4. Identify the significant applications where ITGCs need to be tested.
5. Identify ITGC process risks and related control objectives.
6. Identify the ITGC to test that it meets the control objectives.
7. Perform a reasonable person holistic review of all key controls.
8. Determine the scope of the review and build an appropriate design and effectiveness testing program.

# 8. Get your house in order

The following are the top ten areas to clean up before an IT audit.

1. Establishment of password policies (polices for shared passwords, default passwords, weak passwords, and temporary passwords)
2. De-provisioning and re-provisioning of users (timeliness)
3. Authentication mechanisms implemented on your network
4. Management of existing privileges and roles (or the lack thereof), including:

    - Shared administrative accounts
    - Use of system accounts
    - Use of service accounts

5. Management of event logs and security logs
6. Your user privilege model and the management of changes to group membership and roles:

    - How close is your access control approach to a least privilege model where only the privileges necessary for the change are granted
    - Are policies that segregate duties enforced?
    - Are privileges granted by group membership or by roles?

7. Process for approving elevated privileges
8. Process for granting temporary privileges in production
9. Audit trail of emergency changes to production
10. Audit trail of changes to your company's protected data

Refer to the Appendices for details on how Quest Software can help with these Top Ten Processes.

# 9. Focus on foundational controls

In its April 2006 IT Controls Performance Benchmark Study, the IT Process Institute (ITPI) reported on its examination of 98 IT groups across multiple industries. The study found that out of a full set of 63 IT controls, 21 foundational controls provided most of the benefit.[11] Listed below are the top six foundational controls from that study:

1. Monitoring systems for unauthorized changes
2. Disciplinary policy for intentional unauthorized changes
3. IT configuration management process (including manual and automated)
4. Automation of configuration management
5. Method of tracking successful changes
6. IT infrastructure configuration change notification policy

# 10. Align your controls with your business strategy and goals

Historically, auditors who audited IT infrastructure (below the application layer) focused their efforts on technology and IT security controls in a manner that was often disconnected from the larger business point of view. While they acknowledged that business processes relied on the IT infrastructure, they tended to emphasize risks in the context of technology without considering the larger business context. Likewise, financial auditors have traditionally worked under the assumption that the data housed within the database layer and underlying infrastructure was secure.

Not any more. Today, auditors are not only looking for internal control weaknesses (i.e., unintentionally assumed risks) but for signs of integrated risk management where IT risks are considered in light of business risks. Specifically, IT auditors are looking at the set of controls implemented across the entire IT infrastructure. They are examining whether those controls have been intentionally limited in scope (or prioritized) according to some justification scheme (i.e., intentionally assumed risk), and analyzing the rationale used to justify managing certain controls while omitting others (i.e., justification of assumed risk). As compliance mandates continue to proliferate in this millennium, auditors will accept integrated risk management as not only normative but a basic survival practice.

[11] *Security Controls That Work*, ISACA Control Journal, Vol 4, 2007, pp.29-32.

Here are 10 things that management can do to align IT controls with business goals:

1. Make the corporate compliance attitude explicit, rather than have IT guess what it is. The compliance attitude can be derived from the organization's culture, principles, tone at the top, code of ethics, and risk appetite.
2. Align IT controls to support your organization's corporate compliance posture. Compliance posture should be prominent in the organization's stated corporate strategy, code of conduct, corporate policies, business plan, compliance program, and IT security polices.
3. Make sure you have a defensible risk model for your IT controls.
4. Make sure your enterprise risk model (ERM) includes an IT component. An ERM program will include the integration of historically siloed risk management disciplines including financial, insurance, HR, legal, audit, security, and operations. Make sure the audit, security, and operational risk pieces include an IT component.
5. Make sure your risk model includes both internal and external risks, such as shareholder risks.
6. Make sure your compliance program is "real" for IT (i.e., is a critical success factor in corporate strategies). Specifically, make sure of the following:

    - Your compliance program includes a defensible risk model that accounts for IT risks.
    - IT security policy is active and not gathering dust on a shelf.
    - IT security policy is enforced by including a disciplinary policy for unauthorized changes.

7. Have well-designed controls that are "baked in" (i.e., no "Band-aids").
8. Support automation of IT policies where practical.
9. Develop a process for reviewing recurring control deficiencies to prevent them from constituting a material weakness. Look for trends and root causes.
10. Insist on foundational controls (especially the top six listed in tip #9).

# CONCLUSION

While there are many factors that can influence the outcome of an audit, your level of stress is typically dependent upon five key factors:

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

These five factors can be further distilled into the following keys for reducing audit stress:

- Confidence in your grasp of what's important
- Confidence in the controls operating in the target environment
- A sufficient level of trust established in a working relationship with the auditor

The secret to a stress-free audit is to have all three key factors. Although improving the state of your environment is often considered the top priority, the auditor relationship is actually most important key factor. In the absence of a good relationship with the auditor, you should focus on improving your knowledge, then on your ability to respond, and then on the effectiveness of your internal controls.

# APPENDIX A

## Quest Software and the Top 10 Processes Your IT Auditor Will Want to See

| IT PROCESS | QUEST SOFTWARE SOLUTION |
|---|---|
| Establishment of password policies (polices for shared passwords, default passwords, weak passwords, and temporary passwords) | **Group Policy Manager** provides an advanced version control mechanism for the security management of Active Directory Group Policy Objects (GPOs) across the enterprise.<br>Core aspects of your organizations security policy such as, password policies, logon hours, software distribution and other security settings can be changed, tested, approved and deployed under strict version control allowing you to deploy GPOs in a meaningful and safe manner.<br>**Reporter** collects, stores and reports on data from workstations, Windows servers and Active Directory. Reporter inspects and reveals network occurrences, such as when unauthorized users have administrative rights, when old user accounts should have been deleted or when permissions don't comply with corporate standards.<br>Specifically, Reporter reports on domain password settings such as password expiration dates, domain password policy settings, users with null passwords, password properties, etc |
| De-provisioning and re-provisioning of users (timeliness) | **ActiveRoles Server** can help you manage, automatically provision, re-provision and, more importantly, de-provision users quickly, efficiently and securely in Active Directory, AD LDS (formerly ADAM) and beyond. |
| Authentication mechanisms implemented on your network | **Quest Authentication Services** integrates native Unix and Linux authentication and identity subsystems with Active Directory. It eliminates key vulnerabilities and end-user downtime, to minimize risk and lower costs. |
| Management of existing privileges and roles (or the lack thereof), including:<br>• Shared administrative accounts<br>• Use of system accounts<br>• Use of service accounts | **ActiveRoles Server** provides strictly enforced role-based security, automated group management, change approval and easy-to-use Web interfaces for self service to achieve practical user and group lifecycle management for the Windows enterprise.<br>**Privilege Manager for Unix** protects the full power of root access from potential misuse or abuse. Privilege Manager helps you to define a security policy that stipulates who has access to which root function, as well as when and where individuals can perform those functions. It controls access to existing programs as well as any purpose-built utilities used for common system administration tasks.<br>**Reporter** collects, stores and reports on data from workstations, Windows servers and Active Directory. Reporter inspects and reveals network occurrences, such as when unauthorized users have administrative rights, when old user accounts should have been deleted or when permissions don't comply with corporate standards. |

| IT PROCESS | QUEST SOFTWARE SOLUTION |
|---|---|
| Management of event logs and security logs | **InTrust** collects, stores, reports and alerts on event data from heterogeneous systems, and controls changes to Exchange, AD and GPOs. Using this single solution to manage all platforms reduces the complexity of audit log management, saves expensive storage administration costs, improves information assurance, mitigates risk, and helps to reduce cost and improve efficiency of security, operational and compliance reporting. |
| Your user privilege model and the management of changes to group membership and roles:<br>• How close is your access control approach to a least privilege model where only the privileges necessary for the change are granted<br>• Are policies that segregate duties enforced?<br>• Are privileges granted by group membership or by roles? | **ActiveRoles Server** provides strictly enforced role-based security, automated group management, change approval and easy-to-use Web interfaces for self service to achieve practical user and group lifecycle management for the Windows enterprise.<br><br>**Privilege Manager for Unix** protects the full power of root access from potential misuse or abuse. Privilege Manager helps you to define a security policy that stipulates who has access to which root function, as well as when and where individuals can perform those functions. It controls access to existing programs as well as any purpose-built utilities used for common system administration tasks.<br><br>**InTrust** collects, stores, reports and alerts on event data from heterogeneous systems, and controls changes to Exchange, AD and GPOs. Using this single solution to manage all platforms reduces the complexity of audit log management, saves expensive storage administration costs, improves information assurance, mitigates risk, and helps to reduce cost and improve efficiency of security, operational and compliance reporting.<br><br>**InTrust Plug-in for Active Directory** allows organizations to audit, report, and alert on all domain controller activity, as well as track all detailed changes to Active Directory and Group Policy.<br><br>**InTrust Plug-in for Exchange** allows for detailed, real-time Auditing of Exchange server configurations and permissions. It also provides comprehensive activity tracking and mailbox access for Microsoft Exchange servers<br><br>**InTrust Plug-in for File Access** provides real-time, detailed tracking of all user and administrator activity as it relates to file/object access. With InTrust, this Plug-in for File Access provides efficient collection and storage of audit data and enables organizations to effectively react to, and even prevent, access and permission changes in their file server configurations.<br><br>**Reporter** collects, stores and reports on data from workstations, Windows servers and Active Directory. Reporter inspects and reveals network occurrences, such as when unauthorized users have administrative rights, when old user accounts should have been deleted or when permissions don't comply with corporate standards. |

| IT PROCESS | QUEST SOFTWARE SOLUTION |
|---|---|
| Process for approving elevated privileges | **ActiveRoles Server** provides strictly enforced role-based security, automated group management, change approval and easy-to-use Web interfaces for self service to achieve practical user and group lifecycle management for the Windows enterprise.<br><br>**Quest SafeKeeping** delivers a powerful solution for the management of shared administrative account credentials. When an administrator needs the administrative credential, SafeKeeping ensures security and manageability by providing a secure, automated mechanism for the request, authorization, release, and change of these administrative account logins. |
| Process for granting temporary privileges in production | **ActiveRoles Server** provides strictly enforced role-based security, automated group management, change approval and easy-to-use Web interfaces for self service to achieve practical user and group lifecycle management for the Windows enterprise.<br><br>**Quest SafeKeeping** delivers a powerful solution for the management of shared administrative account credentials. When an administrator needs the administrative credential, SafeKeeping ensures security and manageability by providing a secure, automated mechanism for the request, authorization, release, and change of these administrative account logins. |
| Audit trail of emergency changes to production | **InTrust** collects, stores, reports and alerts on event data from heterogeneous systems, and controls changes to Exchange, AD and GPOs. Using this single solution to manage all platforms reduces the complexity of audit log management, saves expensive storage administration costs, improves information assurance, mitigates risk, and helps to reduce cost and improve efficiency of security, operational and compliance reporting.<br><br>**InTrust Plug-in for Active Directory** allows organizations to audit, report, and alert on all domain controller activity, as well as track all detailed changes to Active Directory and Group Policy.<br><br>**InTrust Plug-in for Exchange** allows for detailed, real-time Auditing of Exchange server configurations and permissions. It also provides comprehensive activity tracking and mailbox access for Microsoft Exchange servers<br><br>**InTrust Plug-in for File Access** provides real-time, detailed tracking of all user and administrator activity as it relates to file/object access. With InTrust, this Plug-in for File Access provides efficient collection and storage of audit data and enables organizations to effectively react to, and even prevent, access and permission changes in their file server configurations. |

| IT PROCESS | QUEST SOFTWARE SOLUTION |
|---|---|
| Audit trail of changes to your company's protected data | **InTrust** collects, stores, reports and alerts on event data from heterogeneous systems, and controls changes to Exchange, AD and GPOs. Using this single solution to manage all platforms reduces the complexity of audit log management, saves expensive storage administration costs, improves information assurance, mitigates risk, and helps to reduce cost and improve efficiency of security, operational and compliance reporting.<br><br>**InTrust Plug-in for Active Directory** allows organizations to audit, report, and alert on all domain controller activity, as well as track all detailed changes to Active Directory and Group Policy.<br><br>**InTrust Plug-in for Exchange** allows for detailed, real-time Auditing of Exchange server configurations and permissions. It also provides comprehensive activity tracking and mailbox access for Microsoft Exchange servers<br><br>**InTrust Plug-in for File Access** provides real-time, detailed tracking of all user and administrator activity as it relates to file/object access. With InTrust, this Plug-in for File Access provides efficient collection and storage of audit data and enables organizations to effectively react to, and even prevent, access and permission changes in their file server configurations. |

# APPENDIX B

# Sample Scheduled Report List

Use this list of scheduled reports (from Quest InTrust) to make your own scheduled report plan for monitoring and managing the IT controls within your environment. As a sign of good intentions (see tip #1), you could even send it to your internal audit department and ask them if there are any they would like to receive on a regular basis.

### Reports to Run against DC (LDAP) (Daily)

Changes to built-in administrative groups membership by Administrative group

Changes to user account passwords by Domain

Computer - All change requests for Active Directory objects by Domain

Computer - Changes to Active Directory object attributes by Domain

Computer objects moved by Domain

Group - All change requests for Active Directory objects by Domain

Group - Changes to Active Directory object attributes by Domain

Group membership management by Domain

Group objects moved by Domain

Group type changed by Domain

Groups created or deleted by Domain

User - All change requests for Active Directory objects by Domain

User - Changes to Active Directory object attributes by Domain

User account options management by Domain

User accounts management by Domain

User accounts moved by Domain

Users created or deleted by Domain

Users disabled or enabled by Domain

## Reports to Run against DC (LDAP) (Weekly)

### AD Changes (user, group, computer)

Changes to built-in administrative groups membership by Administrative Group

Changes to user account passwords by Domain

Computer - All change requests for Active Directory objects by Domain

Computer - Changes to Active Directory object attributes by Domain

Computer objects moved by Domain

Group - All change requests for Active Directory objects by Domain

Group - Changes to Active Directory object attributes by Domain

Group membership management by Domain

Group objects moved by Domain

Group type changed by Domain

Groups created or deleted by Domain

User - All change requests for Active Directory objects by Domain

User - Changes to Active Directory object attributes by Domain

User account options management by Domain

User accounts management by Domain

User accounts moved by Domain

Users created or deleted by Domain

Users disabled or enabled by Domain

### Domain-level Changes

All change requests for GPOs by Domain

Block policy inheritance disabled or enabled by Domain

Changes to Active Directory schema by Object

Changes to assigned Group policy priorities by Container

Changes to Audit Policy settings by Audit Policy

Changes to FSMO roles by Domain

Changes to replication configuration by Forest

Changes to site configuration by Forest

Changes to user rights by Domain

Connection schedule changes

Direct SYSVOL changes by Domain

Domain changes

Domain trust relationship changes

Group Policy assignments by GPO

OU created or deleted by Domain

OU delegation changes

OU moved or renamed by Domain

Permission inheritance changes by Domain

Security options changes by Group Policy

Site link schedule changes

## Reports to Run against DC (Windows Log) (Daily)

Active Directory objects access (Computer)

Active Directory objects access (Group)

Active Directory objects access (User)

All logons (5xx) (Failed)

Computer accounts changes

Group Management

Group Membership Management

Multiple failed account logons (Kerberos 6xx)

Multiple Logon Failures (5xx)

Password resets

User account locked out

User Accounts Management

## Reports to Run against DC (Windows Log) (Weekly)

### AD Changes

- Active Directory objects access (Computer)
- Active Directory objects access (Group)
- Computer accounts changes
- Group Management
- Group Membership Management
- Password resets
- User account locked out
- User Accounts Management
- User rights management

### AD Domain-level Changes

- Audit Policy Changed
- Domain Trusts Changes
- Group Policy Object access
- Kerberos and Domain Policy changed

### Logons

- Account logon events [NT4] (NTLM 6xx) (Failed)
- All logons (5xx) (Failed)
- Multiple failed account logons (Kerberos 6xx)
- Multiple Logon Failures (5xx)

### System

- Event log cleared
- Event Log Errors
- Policy enforcement errors
- Registry Access
- Server reboots [Win2003]
- Server Reboots
- Software installation

# ABOUT QUEST SOFTWARE, INC.

Quest Software, Inc., a leading enterprise systems management vendor, delivers innovative products that help organizations get more performance and productivity from their applications, databases, Windows infrastructure and virtual environments. Through a deep expertise in IT operations and a continued focus on what works best, Quest helps more than 90,000 customers worldwide meet higher expectations for enterprise IT. Quest provides customers with client management as well as server and desktop virtualization solutions through its subsidiaries, ScriptLogic and Vizioncore. Quest Software can be found in offices around the globe and at www.quest.com.

## Contacting Quest Software

| | |
|---|---|
| Phone: | 949.754.8000 (United States and Canada) |
| Email: | info@quest.com |
| Mail: | Quest Software, Inc.<br>World Headquarters<br>5 Polaris Way<br>Aliso Viejo, CA 92656<br>USA |
| Web site: | www.quest.com |

Please refer to our Web site for regional and international office information.

## Contacting Quest Support

Quest Support is available to customers who have a trial version of a Quest product or who have purchased a commercial version and have a valid maintenance contract. Quest Support provides around the clock coverage with SupportLink, our web self-service. Visit SupportLink at http://support.quest.com

From SupportLink, you can do the following:

- Quickly find thousands of solutions (Knowledgebase articles/documents).
- Download patches and upgrades.
- Seek help from a Support engineer.
- Log and update your case, and check its status.

View the ***Global Support Guide*** for a detailed explanation of support programs, online services, contact information, and policy and procedures. The guide is available at: http://support.quest.com/pdfs/Global Support Guide.pdf