

Realtime
publishers

"Leading the Conversation"

The Shortcut Guide[™] To



Improving IT Service Support through ITIL

sponsored by



i n v e n t

Rebecca Herold

Chapter 4: Supporting Compliance Through ITIL	62
IT Compliance Is Relatively Young	62
Frameworks Support Compliance.....	63
ITIL Has Been Validated.....	64
ITIL Service Management Supports Compliance.....	64
SOX Mapping to ITIL Service Management.....	65
ITIL Supports Compliance with Many Laws and Regulations	67
Compliance with Policies and Procedures	68
ITIL Supports Compliance and Improves Business	69
Change Management	70
Incident Management.....	72
Problem Management	73
Compliance Requires Accountability—ITIL Establishes Accountability	75
Summary	75

Copyright Statement

© 2007 Realtimepublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimepublishers.com, Inc. (the “Materials”) and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED “AS IS” WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimepublishers.com, Inc or its web site sponsors. In no event shall Realtimepublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimepublishers.com and the Realtimepublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimepublishers.com, please contact us via e-mail at info@realtimepublishers.com.

[**Editor's Note:** This eBook was downloaded from Realtime Nexus—The Digital Library. All leading technology guides from Realtimepublishers can be found at <http://nexus.realtimepublishers.com>.]

Chapter 4: Supporting Compliance Through ITIL

Organizations have faced legal and regulatory requirements for literally decades. Perhaps the first, most painfully apparent compliance requirements were experienced by U.S. businesses in 1970. At that time, there was huge concern about the increasingly large numbers of deaths and injuries that occurred at work sites. A new oversight agency, the Occupational Safety and Health Administration (OSHA), was created in 1970 and tasked to create regulations to ensure worker safety. Businesses hated these directives. Many business leaders predicted that following the new safety regulations would cost businesses huge amount of money not only because of lost productivity but also because of how much just getting into compliance would cost. Many of the requirements seemed unnecessary based solely upon the cost and time involved for their implementation. However, history has shown that, as a result of OSHA requirements and compliance by organizations, there have been measurably fewer injuries and deaths and significantly less lost work. In addition, there have been fewer workers' compensation losses.

IT Compliance Is Relatively Young

Fast forward a couple of decades and, as Yogi Berra would say, "It's *deja vu* all over again." U.S. healthcare organizations reacted with alarm over the passage of the Health Insurance Portability and Accountability Act (HIPAA) of 1996. The U.S. financial organizations soon followed suit with their reaction to the passage of the Gramm Leach Bliley Act (GLBA), also known as the Financial Modernization Act, of 1999. But probably the biggest whammy felt by the largest numbers of organizations was felt by passage of the Sarbanes Oxley (SOX) Act of 2002. There have been many data protection laws that have been enacted since around 1995 throughout the world. Organizations now must follow specific requirements to protect information and the IT infrastructures that process and house the data.

In addition to these laws, there is now a new trend to require organizations that perform certain activities, such as processing credit cards, to have very specific data protection practices implemented. The perfect example of this is the Payment Card Industry (PCI) Data Security Standard (DSS). Although this standard is not a law, it is a contractual requirement for processing credit cards from Visa, MasterCard, American Express, and others.

Protecting information is no longer just a good idea; it is a legal requirement that is best accomplished by using proven, internationally accepted, data management frameworks.

Frameworks Support Compliance

Some of the current prominent frameworks for IT and information security governance are ITIL, COBIT, ISO/IEC 17799 (soon to be ISO27002), and COSO.

 Recall each of these? Let's quickly review:

Information Technology Infrastructure Library (ITIL) offers best practice approaches to facilitate the delivery of high-quality information technology (IT) services, the earliest version of which was released in 1985.

Control Objectives for Information and related Technology (COBIT) provides best practices for IT management and controls created by the Information Systems Audit and Control Association (ISACA) and the IT Governance Institute (ITGI) in 1992.

ISO/IEC 17799 is an information security standard most recently published in June 2005 by the International Organization for Standardization (ISO) and the International Electrotechnical Commission (IEC). This standard was renumbered ISO/IEC 27002:2005 in July 2007.

Committee of Sponsoring Organizations (COSO) of the Treadway Commission is a U.S. private-sector initiative formed in 1985 that makes recommendations to reduce fraud incidents. COSO has a common definition of internal controls, standards, and criteria against which companies and organizations can assess their control systems.

There has been much written in the past few years about ITIL. Why? Because ITIL is a perfect complement to both COBIT and ISO/IEC17799. It aligns nicely with them. ITIL, COBIT, and ISO/IEC 17799 interoperate in many ways. Most organizations that use frameworks will typically use more than one; they realize that just one framework does not address all the issues necessary for effective information management within a complex business environment.

With the passage of SOX, it has been common to see organizations use COSO and COBIT in conjunction with ITIL. Auditors overwhelmingly use COBIT to determine appropriate controls when doing SOX reviews. IT areas can benefit from following a standardized framework, such as ITIL, to support COBIT constructs, and at the same time ensure SOX compliance. Why is this? Because COBIT and ITIL provide frameworks covering the areas that must be reviewed, along with the necessary criteria to use for evaluations, when considering the effectiveness of IT service management.

 It is important to keep in mind that COBIT and ITIL do not provide explicit solutions to the risks being discussed within them. For them to try to do so would be foolhardy considering the very wide range of technology solutions that exist along with the technologies emerging every day. However, COBIT and ITIL—which address general and significant IT control and management issues in basically all organizations—provide an efficient and effective roadmap to follow to successfully implement IT solutions. Because COBIT and ITIL include what are widely accepted as best practices, the documentation and implementation of the concepts will provide the best possible, and defensible, IT management results.

ITIL Has Been Validated

The concepts within frameworks have been tried and tested within numerous organizations, and they work! Frameworks are efficient and effective. Frameworks already exist; you do not need to create something from scratch yourself. You don't need to spend staff and management time creating roughly similar processes—after numerous trials and errors—that may not be as effective as these already existing frameworks. Frameworks can offer a competitive advantage.

ITIL offers cost savings, efficiency, and a competitive advantage. Why? The following list highlights just a few of the reasons:

- ITIL satisfies and extends COBIT controls relating to IT Service Management, including Change Management, Problem Management, and Incident Management.
- ITIL improves IT processes and controls. The organizations that have successfully implemented ITIL attest to that.
- ITIL can be used to determine technology requirements and identify possible organizational structure, roles, and responsibilities.
- ITIL Service Support processes enable effective IT services and contain the building blocks of all IT services.
- ITIL is increasingly being used to implement the best practices promoted by COBIT and ISO/IEC 17799.

ITIL Service Management Supports Compliance

ITIL supports compliance with many laws and regulations, such as the USA PATRIOT Act, California SB1386, SOX, the European Union Data Protection Directive 95/46/EC, Basel II, GLBA, HIPAA, the U.S. state breach notice laws, and many more. However, actual ITIL specifications do not contain references to any particular regulations or laws; there would be too many to list, and too many new ones are going into effect. By comparing the requirements of various laws and regulations, though, it becomes clear how ITIL supports compliance.

Data protection and privacy laws and regulations throughout the world have many commonalities, and they promote following accepted best practices and standard frameworks. In fact, by following frameworks such as COSO, COBIT, ISO/IEC 17799, and ITIL, organizations will realize compliance with roughly 80% to 85% of the data protection requirements within all these many laws and regulations.

Much more time will be spent on compliance activities if they are addressed in an ad-hoc manner or with one-off solutions. By following defined frameworks, much time and resources will be saved in meeting compliance objectives. Using a well-defined framework allows for a comprehensive approach to compliance.

SOX Mapping to ITIL Service Management

It is important to note that standard auditor recommendations are based upon these widely respected and internationally endorsed IT and information security frameworks. Why? Because regulatory oversight agencies reference the use of these frameworks over and over again within their compliance guidance documents.

Just consider SOX. SOX gave the Public Company Accounting Oversight Board (PCAOB) responsibility for oversight of SOX compliance. The PCAOB then created several guidance documents to help auditors and organizations determine whether organizations had proper controls in place.

 PCAOB "is a private-sector, non-profit corporation, created by the Sarbanes-Oxley Act of 2002, to oversee the auditors of public companies in order to protect the interests of investors and further the public interest in the preparation of informative, fair, and independent audit reports." For more information, see their Web site at <http://www.pcaobus.org/>.

The PCAOB recommends the COSO and COBIT frameworks be used to meet SOX compliance within various guidance documents they have issued, such as in PCAOB Release No. 2004-001, March 9, 2004, and in their Auditing Standard #2. The PCAOB directed that established frameworks be used by organizations to support consistent and effective internal controls.

So, SOX directed the PCAOB to create guidance, and the PCAOB mandated the use of established and effective frameworks for internal controls. ITIL clearly maps to COBIT and COSO. Figure 4.1 demonstrates these relationships.

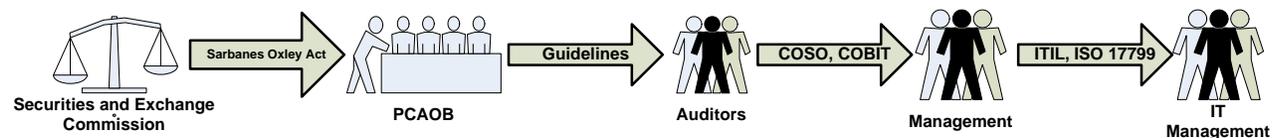


Figure 4.1: How SOX relates to ITIL.

Now let's drill down a little further to the point where the auditors are using COBIT to evaluate your IT controls. Auditors will use the COBIT 4.0, Manage Changes (AI6, AI7) section. The Control Objective is "Controls provide reasonable assurance that system changes of financial reporting significance are authorized and appropriately tested before being moved to production."

What does this have to do with financial reporting controls? The Rationale explains it well:

Managing changes addresses how an organization modifies system functionality to help the business meet its financial reporting objectives. Deficiencies in this area could significantly impact financial reporting. For instance, changes to the programs that allocate financial data to accounts require appropriate approvals and testing prior to the change so that proper classification and reporting integrity is maintained.

This relates to Section 404 of SOX general requirements because they are there to ensure proper internal controls exist for processes, automation, and documentation. IT managers, internal auditors, controllers, process specialists, and IT systems personnel are accountable for ensuring these controls exist.

Figure 4.2 shows at a high level how ITIL Service Management processes support SOX Section 404. Details for each are discussed later in the chapter.

Change Management	Incident Management	Problem Management
Requests for program changes, system changes, and maintenance (including changes to system software) are standardized, logged, approved, documented, and subject to formal change management procedures	IT management has defined and implemented a incident management system such that data integrity and access control incidents are recorded, analyzed, resolved in a timely manner and reported to management	The problem management system provides for adequate audit trail facilities, which allow tracing from incident to underlying cause
Emergency change requests are documented and subject to formal change management procedures	A security incident response process exists to support timely response and investigation of unauthorized activities	
Controls are in place to restrict migration of programs to production by authorized individuals only		
IT management implements system software that does not jeopardize the security of the data and programs being stored on the system		
Rapid disclosure of operations, financial reporting and compliance validation and documentation		

Figure 4.2: How ITIL Service Management supports SOX Section 404 requirements.

The general ITIL controls that support all three of these IT Service Management processes include:

- Application controls, such as those for the systems development life cycle (SDLC), logging access activities, and processing and reporting financial activities of all types
- IT general controls, such as access controls, authorization, and records retention
- Document controls, such as the existence of policies, procedures, narratives, flowcharts, configurations

ITIL Supports Compliance with Many Laws and Regulations

As Figure 4.3 highlights, ITIL supports compliance with many other laws and regulations. Later, this chapter will delve deeper into the specifics of how ITIL Change Management, Incident Management, and Problem Management support compliance with these legal requirements.

Law or Regulation	Requirements Supported by ITIL
Basel II	Monitoring and reporting; internal controls; risk management; documentation; and accountability
GLBA	Detecting, preventing and responding to attacks, intrusions, or other systems failures; testing and monitoring; assigning security and privacy responsibility; providing policies and procedures for access controls; developing an awareness and training program
HIPAA	Providing policies and procedures to prevent, detect, contain, and correct security violations; assigning security and privacy responsibility; offering policies and procedures for access controls; developing an awareness and training program; ensuring there are policies and procedures for responding to an emergency; implementing audit controls, authentication controls, and incident response
European Union Data Protection Directive 95/46/EC	Ensuring data accuracy; providing access controls; assigning responsibility; ensuring data retention
Canada's Personal Information Protection and Electronic Data Act (PIPEDA)	Providing access controls; ensuring data retention and data accuracy
U.S. State Breach Notice Laws	Implementing incident response; assigning accountability

Figure 4.3: Laws and regulations ITIL supports.

Compliance with Policies and Procedures

In addition to complying with laws and regulations, you must comply with your own organization's policies. Unfortunately, too many organizations do not realize this. The security and privacy policies posted on an organization's Web site are legally binding documents. Do you have procedures in place within your organization to support compliance with them?

Auditors and regulators will review your organization's internal information security and privacy policies to determine whether your organization is following the policies. Do you have procedures to support compliance with your policies?

Most organizations have documented policies but do not offer documented procedures to support compliance, and very little to no training and awareness to communicate those policies to personnel and business partners. All organizations within the U.S. that are in noncompliance of their policies are putting themselves at risk of being found in violation of the U.S. Federal Trade Commission Act (FTC Act). Section 5 of the FTC Act declares that unfair or deceptive trade practices are illegal. Not following your own policies is generally considered as an unfair and deceptive trade practice. Not following your policies, which are basically the promises you make to your customers and employees, is considered misleading your consumers. This may be in the form of express or implied claims or promises, and may be written or oral.

A few examples of organizations that have received fines and penalties as a result of noncompliance with their own policies include:

- In May 2007, the FTC found Pacific Herbal Sciences to be in violation of the FTC Act and were fined \$172,500. The FTC contended that the defendants falsely claimed on their Web site ordering pages that transactions were secure and that customer privacy was protected. The Web site contained the message, "NOTE: To ensure your personal privacy, all of the information that you submit to us after this point will be secured using SSL encryption technology." However, the transactions were not secured in this manner.
- In November 2006, the FTC applied a \$3 million penalty against Zango Inc. for their unfair and deceptive business practices because they did not have procedures in place to support their policies.
- In September 2006, the FTC fined Enternet \$2 million for being in violation of the FTC Act for misleading consumers with their privacy policies.



It is important to note that the FTC also typically requires violators of the FTC Act to establish formal information security programs and undergo ongoing independent audits of the adequacy of the programs for a period of 20 years. The ongoing purview of the FTC is often more expensive than the dollar penalty.

ITIL Supports Compliance and Improves Business

ITIL Change Management, Incident Management, and Problem Management processes support compliance with laws, regulations, and corporate policies. In addition to supporting compliance, implementing these ITIL processes will result in:

- Cost justification for service quality activities
- Better integration of corporate processes
- Better integration of IT with other business processes throughout the enterprise
- Support for systems audits
- Creation of key performance indicators
- Documented roles and responsibilities in service provisioning
- Enhanced efficiency, resulting in better competitiveness
- Improved availability, reliability, and security of mission-critical IT services
- Improved resource utilization
- Improved process scalability and consolidation
- Improved project deliverables and time to delivery
- Continuous learning process and feedback
- Reduced rework and elimination of redundant work
- Services better able to meet business, customer, and user demands

So, with all these in mind, let's look at the details for how these three ITIL Service Management processes support not only compliance but also business improvement.

Change Management

One of the key internal control objectives in COBIT is managing change. Managing change is also one of the required General IT controls. The foundation of an effective and efficient IT control environment is effective Change Management.

Well-defined documented processes based on best practices frameworks, such as ITIL, and supported by automation where possible, are necessary to achieve compliance. The following Change Management activities support compliance requirements:

- Ensuring system changes are authorized and appropriately tested before being moved to production
- Having a documented change management process and keeping it maintained to reflect the current process
- Having change management procedures for all changes within the production environment, including program changes, system maintenance, and infrastructure changes
- Following procedures to control and monitor change requests
- Following procedures to initiate, approve, and track change requests
- Following documented procedures to appropriately test and approve changes before placing them into production
- Ensuring the approval procedures address all the following: operations, security, IT infrastructure management, and IT management
- Following documented procedures to ensure only authorized/approved changes are moved into production
- Maintaining an audit trail, change request log, and supporting documentation
- Ensuring documented procedures for timely implementation of patches to system software
- Maintaining and following documented procedures to control and supervise emergency changes
- Maintaining an audit trail of all emergency activity and following procedures to have it independently reviewed
- Following documented procedures, including back out activities, for emergency changes
- Following documented procedures to ensure all emergency changes are tested and appropriately approved by systems owners, development staff, and computer operations, as appropriate, before being put into production
- Establishing separation of duties between the staff responsible for moving a program into production and development staff
- Following documented procedures to perform a risk assessment of the potential impact of changes to system software

The benefits of following the ITIL Change Management process go beyond compliance. The organizational benefits include:

- Cost savings—According to Nouri Association, Inc. (NAI), organizations save 30% to 50% using frameworks with automated controls compared with those that use manual change management controls.
- Increased customer satisfaction—Change management occurs more consistently and dependably. Customers know the status of their change request throughout the entire change process.
- Production environment stability—NAI research shows there is a 15% to 20% decrease in change-related incidents.
- Supports quality assurance (QA) initiatives—Following the structured, well-documented, and consistent processes within ITIL Change Management supports QA recommendations, such as those found within Six Sigma.

To most efficiently and effectively handle IT changes and compliance requirements, the Change Management process should be centrally managed and integrated throughout the entire applications and SDLC. Activities that should be centrally managed to process changes include:

- Recording—Ensuring all change sources can submit requests for change (RFCs) and that the RFCs are properly recorded
- Acceptance—Filtering submitted RFCs and moving those eligible on for consideration
- Classification, categorization, and prioritization—Putting each RFC into the appropriate category and establishing a priority
- Planning and approval—Consolidating the changes, giving approvals, obtaining resources, and involving the change advisory board (CAB) where necessary
- Coordination—Scheduling, development, testing, and implementation
- Evaluation and closure—Determining success and learning from the experience

Incident Management

The Incident Management process needs to manage all incidents from detection and recording through to resolution and closure. Incident Management is reactive by nature. The objectives of Incident Management are to reduce or eliminate the business impacts and effects of actual or likely disturbances within IT services to not only ensure personnel can get back to work as soon as possible but also that business can resume to normal as soon as possible.

Another COBIT internal control objective is managing incidents. The following Incident Management activities also support compliance requirements:

- Documenting and maintaining a formal incident management system.
- Establishing and maintaining formally documented incident management procedures.
- Providing training for, and consistently following, incident management procedures.
- Obtaining clearly documented management support for incident management processes.
- Establishing consistent, well-documented incident reports that include information about the incident, how the incident was analyzed, and how it was resolved.
- Establishing incident management audit trails to track the entire incident resolution lifecycle, from initial report to confirmed resolution.
- Establishing procedures to respond to unauthorized activities in a timely manner.

Well-defined documented procedures, automated where possible, help to further support compliance. Automation helps to ensure procedures are consistently and completely followed and reduce the amount of human error. The types of activities that occur within Incident Management that can be automated to support compliance requirements include:

- Incident acceptance and recording—Detecting and reporting an incident and then creating an incident record
- Classification and initial support—Assigning the incident a type, status, impact, urgency, priority, service level agreement (SLA), and so on to help facilitate the most appropriate response; this should include providing temporary workarounds whenever applicable
- Service request—Documenting and implementing automated procedures to request IT services whenever necessary to support incident response
- Matching—Determining whether the incident is known and if there is a workaround in place

- Investigation and diagnosis—Determining whether a known solution to an incident does not exist, then following procedures to launch an investigation
- Resolution and recovery—Following procedures to find a solution, documenting it, and then automatically notifying the appropriate individuals and areas
- Closure—Upon obtaining confirmation from those notified that the solution is satisfactory, following automated procedures to formally close the incident
- Progress monitoring and tracking—Throughout the incident response life cycle, monitoring progress so that the time it takes to resolve the incident is recorded; in addition, ensuring that, when roadblocks occur, that incident is appropriately escalated to the next level of support.

Problem Management

So how is a problem different than an incident? As I discussed in Chapter 1, a problem is generally an unwanted or undesirable situation that, if not addressed soon enough, can become the root cause of an incident. Problem Management takes the entire IT infrastructure into account, using all available information, to identify existing and potential failures in the delivery of IT services.

Problem Management supports Incident Management by providing alternative workarounds and temporary fixes during an incident but does not have responsibility for actually resolving incidents. Problem Management also involves the analysis of incidents and problems to identify trends and then subsequently takes proactive actions to prevent the further occurrences of similar incidents and problems.

Problem Management also supports COBIT internal control objectives and, as a result, compliance with laws and policies. The following Problem Management activities support compliance requirements:

- Establishing a documented Problem Management system and ensuring it is being used throughout the enterprise
- Establishing formally documented procedures to use the Problem Management system, including consistent reports and review practices
- Following formally documented procedures to create audit trails for Problem Management activities

Well-defined documented Problem Management procedures, automated where possible, help to further support compliance. As with Incident Management, automation helps to ensure procedures are consistently and completely followed and reduce the amount of human error. The types of activities that occur within Problem Management that can be automated to support compliance requirements include:

- Problem identification and recording—Automating problem reporting helps to streamline the identification of known and new problems, in addition to supporting better trend analysis.
- Problem classification and allocation—Determining the category, impact, urgency, priority, and status of a problem then allocating resources for resolution is made more efficient through automation.
- Problem investigation and diagnosis—Determining the cause of the problem and linking it to the appropriate CIs is more accurate and time efficient through automation.
- Temporary fixes—Implementing necessary temporary or emergency fixes to manage known errors until they can be resolved is accomplished much more quickly by using automated processes to identify the temporary fixes.
- Error identification and recording—Identifying the error and then communicating the error to Incident Management, if appropriate, is made easier through automation.
- Error assessment—Determining what is necessary to resolve known problems and errors is made easier through automation.
- Record error resolution—Determining the most appropriate business solution is done more quickly through automation.
- Close error and associated problems—Performing a Post Implementation Review (PIR) and then closing the records is done more accurately and efficiently through automation.

Compliance Requires Accountability—ITIL Establishes Accountability

Another key aspect of achieving compliance is establishing accountability. When management visibly supports and takes ownership of the organization's IT control strategy, accountability is achieved. In IT, control strategy is composed of three types of interrelated controls, all of which support compliance and are a result of implementing ITIL:

- Preventive controls help keep bad and unauthorized things from happening. Examples of preventive controls are policy, segregation of duties, and authorization processes. Compliance requires all these controls. ITIL establishes these controls.
- Detective controls are analytical controls that monitor activities and processes to identify when preventive controls have failed or been circumvented. Examples of detective controls include change auditing and post-deployment verification of changes to the production infrastructure. Compliance requires all these controls. ITIL establishes these controls.
- Corrective controls restore the IT environment to an authorized and appropriate state when the detective controls identify something that is not appropriate. Examples of corrective controls include restoring programs and provisioning tools. Compliance requires all these controls. ITIL establishes these controls.

An effective IT control strategy will utilize all these controls and be designed to minimize risk to the business. By implementing these controls following ITIL, regulatory and policy compliance in large part can be achieved.

Summary

As organizations continue to look for better ways to manage IT while meeting regulatory and policy compliance, ITIL continues to grow in popularity. As a result, organizations also realize better integration of IT throughout all enterprise business processes.

Putting ITIL in place requires careful planning and commitment, and it is usually expensive. ITIL is often best implemented with other frameworks, particularly COBIT, to meet compliance requirements. However, organizations that take a proactive approach to compliance and frameworks implementation realize they also achieve greater efficiency, reduced operational and legal risk, and lower operational expense.

According to studies of high-performing IT organizations by the IT Process Institute, implementing frameworks as part of their compliance efforts spent less than 10 full-time equivalent (FTE) staff-years on SOX Section 404 activities compared with hundreds of FTEs in other organizations. The organizations working towards frameworks and compliance goals spent less than 5% of their time on IT problem resolution compared with 35% to 45% spent on unplanned, unscheduled work in other IT organizations that were not using frameworks [Behr, K., G. Kim, and G. Spafford, *The Visible Ops Handbook*, Information Technology Process Institute (ITPI), 2004-2005]. ITIL implementation continues to grow throughout the world; a reminder of the growing importance of international standards.

When you are implementing controls and processes to meet compliance requirements so that you can avoid litigation, fines, and penalties under your applicable laws and policies, take the opportunity to also act strategically to incorporate IT throughout all your organization's business decision-making processes. You will find that taking this risk-based, frameworks approach will create valuable benefits beyond compliance. You will see that the resulting strong IT controls strategy will achieve compliance objectives as well as increase IT efficiency and effectiveness.

Download Additional eBooks from Realtime Nexus!

Realtime Nexus—The Digital Library provides world-class expert resources that IT professionals depend on to learn about the newest technologies. If you found this eBook to be informative, we encourage you to download more of our industry-leading technology eBooks and video guides at Realtime Nexus. Please visit <http://nexus.realtimepublishers.com>.