

Change and Patch Management Controls: Critical for Organizational Success





Know anyone
with change
control issues?

TRIPWIRE

Audit Change. Prove Control.

"Tripwire is one of our most valuable tools to assure once and future compliance."

—Barak Engle, CSO, InStorecard



In the age of Sarbanes-Oxley, practically every company is discovering their IT change and configuration management tools and other process improvements aren't enough to prove compliance. They need something more. They need Tripwire.

Tripwire is the antidote for out-of-control change. Our change auditing solutions specifically address enterprise needs for independent detective controls. We give you a single point of control for detecting, reconciling and reporting change activity across servers, desktops, network devices, and other infrastructure components.

Find out why more than 4000 customers rely on Tripwire to achieve compliance in a wide range of regulatory environments. Sign up for our webcast, *Sorting out SOX*, at www.tripwire.com/iia.

CONTROL. COMPLIANCE. CONFIDENCE.

IT GOVERNANCE

Today's organizations are faced with a growing number of corporate and IT governance requirements, many of which leverage the same general IT controls.

With BMC Software, you can implement systems-based IT controls to automate the most challenging control activities and realize a significant return on investment by improving operational efficiency, reducing costs and driving productivity throughout your organization.

Let BMC Software help you get started on the road to compliance and control. Our best practice solutions can help you automate IT general controls in the areas of:

- Identity and Access Management Controls
- Data Management and Recovery Controls
- Change and Configuration Controls

Our solutions support the best practices of the IT Infrastructure Library (ITIL®) framework and the control objectives of COBIT. Now you can share the benefits of more than 15,000 BMC Software customers worldwide.

It's not just about regulatory compliance—it's about proactively managing your business from the top down.

Learn more at www.bmc.com/compliance

Sarbanes-Oxley

Basel II

Six Sigma

COBIT

ITIL®

eTOM

BS 15000



*The Institute of Internal Auditors
Global Technology Audit Guide
Change and Patch Management Controls: Critical for Organizational Success*

Authors:

*Jay R. Taylor, General Motors Corp.
Julia H. Allen, Carnegie Mellon University, Software Engineering Institute
Glenn L. Hyatt, General Motors Acceptance Corp.
Gene H. Kim, Tripwire Inc.*



This guide has been produced and distributed through
the sponsorship of BMC Remedy and Tripwire.



AICPA – American Institute of
Certified Public Accountants
www.aicpa.org



CIS – Center for Internet Security
www.cisecurity.org



CMU/SEI – Carnegie-Mellon University
Software Engineering Institute
www.cmu.edu



ISSA – Information Systems Security Association
www.issa.org



NACD – National Association of
Corporate Directors
www.nacd.org



SANS Institute
www.sans.org

Section 1	
Summary for the Chief Audit Executive	1
Section 2	
Introduction	4
Section 3	
Why Should I Care About the Way My Organization Is Managing Change?	9
Section 4	
Defining IT Change Management	13
Section 5	
What Questions Should I Ask About Change and Patch Management?	20
Section 6	
Three Months Later: Sydney's Story Concludes	24
Section 7	
Where Should Internal Auditors Begin?	27
Section 8	
Where Can I Learn More?	30
Section 9	
Appendix A: IT Change Management Audit Program.....	31
Section 10	
Appendix B: The Visible Ops Methodology	38
Section 11	
Appendix C: Example Business Case for Change Management	39
Section 12	
Appendix D: Change Management Tools and Vendors	41
Section 13	
References	42
Section 14	
About the Authors	43
Section 15	
Sponsor Profiles	44

GTAG — List of Figures and Tables

List of Figures

Figure 1: COSO ERM Model for Change Management.....	12
Figure 2: Unplanned Work as Indicator of Effective Change Management Processes	18
Figure 3: Key Variables That Influence Change Management Processes	18
Figure 4: Change Management Capability Levels	23

List of Tables

Table 1: Change Management Metrics	16
Table 2: Questions to Ask About Change Management by Archetype	20
Table 3: IT Change Management Audit Program	32
Table 4: Typical Roles	37
Table 5: Segregation of Duties	37
Table 6: Issues and Indicators of Ineffective Change Management.....	39
Table 7: Benefits From Effective Transformation	39

1.1 Why the CAE Must Be Involved in Controlling Change and Patch Management

You may be wondering why you should read a guide on the subject of information technology (IT) change and patch management. After all, isn't this something you can completely delegate to your technical IT audit staff? And isn't there sufficiently thorough guidance on this topic that goes back to managing the mainframe environment? The short answer to both of these questions is "no."

While the primary role of chief audit executives (CAEs) does not include being experts on technology, significant risks exist around virtually all business uses of technology. It is important to understand that you do not need to be an expert to help people manage technology and its associated risks. The goal of this guide is to help CAEs, their executive peers, and staff enhance their knowledge associated with technology management, and help them counsel management on governing these processes effectively.

For the intended audience of this guide, issues related to IT change control rarely have been as important as they are now. CAEs are being held accountable by audit committees and are expected to comply with regulations such as the U.S. Sarbanes-Oxley Act of 2002 Section 404. Having the knowledge to effectively challenge IT management is not only useful, but essential.

After reading this guide, you will:

- Have a working knowledge of IT change management processes.
- Be able to distinguish quickly great change management processes from ineffective ones.
- Be able to recognize quickly red flags and indicators that IT environments are having control issues related to change management.
- Understand that effective change management hinges on implementing preventive, detective, and corrective controls to enforce segregation of duties and ensuring adequate management supervision.
- Be in a position to recommend the best known practices for addressing these issues, both for assurance on risks (including controls attestations), as well as increasing effectiveness and efficiency.
- Be able to sell your recommendations more effectively to your chief information officer (CIO), chief executive officer (CEO), and/or chief financial officer (CFO).

Because every "IT risk" creates some degree of business risk, it is important that CAEs thoroughly understand change management issues.

Change and patch management is defined here as the set of processes executed within the organization's IT department designed to manage the enhancements, updates, incremental fixes and patches to production systems, which include:

- Application code revisions.
- System upgrades (applications, operating systems, databases).

- Infrastructure changes (servers, cabling, routers, firewalls, etc.).

Collectively, we refer to these as "IT changes." All organizations have to deal with IT changes effectively, because virtually every business decision requires one or more changes to assets. When changes fail or are poorly controlled, the impact on the business can range from minor inconvenience to events that hinder the achievement of business objectives, including the ability to comply with the growing body of regulation.

1.2 Poor Change Management Can Be Identified Quickly

This guide was developed to help CAEs ask the right questions of the IT organization to assess its change management capability. To help you quickly assess the overall level of process risk and determine whether a more detailed process review may be necessary, this guide also provides expected answers to these questions.

Top Five Risk Indicators of Poor Change Management:

- *Unauthorized changes (above zero is unacceptable).*
- *Unplanned outages.*
- *Low change success rate.*
- *High number of emergency changes.*
- *Delayed project implementations.*

This guide includes field-tested metrics to help you assess the health of the change management process quantitatively, as well as suggested management metrics to guide your organization to achieve and sustain higher levels of control and performance. In this way, internal auditors can assist management by identifying the sources of risk to the organization and assessing the effectiveness of risk management, governance, and control processes.

Easily recognizable symptoms and indicators of control failures due to poorly controlled IT changes include:

- Unavailability of critical services and functions, even for short periods of time.
- Unplanned system or network downtime, halting execution of critical business processes such as coordinating schedules with suppliers and responding to customer orders.
- Downtime on critical application, database, or Web servers, preventing users from performing their critical tasks.
- Negative publicity and unwanted board attention.

At an organizational level, indicators that IT organizations may have systemic change management control issues include:

- Majority of the IT organization's time is spent on operations and maintenance (>70 percent) instead of helping the business in deploying new capability.
- Failure to complete projects and planned work (due to high amounts of firefighting and unplanned work).

- IT management is being awakened in the middle of the night regarding problems.
- High IT staff turnover.
- Adversarial relationships between IT support staff, developers, and business customers (internal or external), usually over poor service quality or late delivery of functionality.
- High amounts of time required for IT management to prepare for IT audits and to remediate the resulting findings.

.....
Many organizations are just one change away from being a poor performer.
.....

1.3 Understanding How IT Change Is Managed Effectively

Change management is sometimes difficult for organizations to master because so many stakeholders are involved (e.g., business managers, application system developers, IT operations staff, auditors). However, this is not a reason for organizations to be complacent about inadequate controls or low performance.

Stable and managed production environments require that implementation of changes be predictable and repeatable, following a controlled process that is defined, monitored, and enforced. The necessary IT controls to achieve this are analogous to the controls used in financial processes to reduce the risk of fraud and errors: segregation of duty controls (which are preventive in nature) and supervisory controls (which are preventive and detective in nature). [Chambers 03]

CAEs will be very familiar with these controls: Only the minimal staff required to implement IT production changes should have access to the production environment (preventive). Authorization processes should involve stakeholders to assess and mitigate risks associated with proposed changes (preventive). Supervisory processes should encourage IT management and staff to undertake their duties responsibly (preventive), and be able to detect errant performance (detective).

Donna Scott, vice president and research director, Gartner, notes that “80 percent of unplanned [IT] downtime is caused by people and process issues, including change management practices.” These issues arise in the absence of automated preventive, detective, and corrective controls that enable good risk-based decisions around change and effective monitoring and enforcement of the change management process.

High-performing IT organizations also have reached this conclusion, which is supported by extensive work performed by the Software Engineering Institute (SEI) and the IT Process Institute (ITPI).

What do all high-performing IT organizations have in common? They have a culture of change management that

prevents and deters unauthorized change. They also “trust but verify” by using independent detective controls to reconcile production changes with authorized changes, and by ruling out change first in the repair cycle during outages. Finally, they also have the lowest mean time to repair (MTTR).

Auditors will appreciate that in these high-performing IT organizations, change management is not viewed as bureaucratic, but is instead the only safety net preventing them from becoming a low-performer. In other words, IT management owns the controls to achieve its own business objectives, efficiently and effectively.

.....
Achieving a change success rate over 70 percent is possible only with preventive and detective controls.
.....

Internal auditors, together with management, want to ensure change management-related risks have been identified and are being measured and managed properly. The key point to remember is that change management requires focusing on process with a managerial and human focus, and is supported with technical and automated controls.

1.3.1 Regulatory Considerations

Effective change management processes can assist the organization in maintaining ongoing compliance with new and expanding regulations. Particular care must be exercised when implementing changes to technology that supports the financial reporting process. Such changes can impact organizational compliance with Sarbanes-Oxley, the European Union privacy directives, and State of California Senate Bill (SB) 1386 requirements. Uncontrolled changes in production can lead to errors that, if pervasive or critical, could be considered significant deficiencies. Where key financial controls are impacted or the organization has failed to correct significant IT general control deficiencies identified in the prior year (such as in change management), management may face the possibility of having to deal with material weaknesses.

.....
When Failure Is Not an Option

By managing changes, you manage much of the potential risk that changes can introduce.
.....

1.4 The Top Five Steps to Reduce IT Change Risks

In this guide, we have framed the observed best known practices of change management processes that reduce business risk and increase IT efficiency and effectiveness. In summary, five prescriptive steps that can be taken immediately by most organizations to improve their change management processes are:

- Create tone at the top motivating the need for a culture of change management across the enterprise, supported by a declaration from IT management that the

only acceptable number of unauthorized changes is zero. Preventive and detective controls can then be put in place to help achieve and sustain this objective, ensuring that all production changes can be reconciled with authorized work orders.

- Continually monitor the number of unplanned outages, which is an excellent indicator of unauthorized change and failures in change control.
- Reduce the number of risky changes by specifying well-defined and enforced change freeze and maintenance windows. This maximizes stability and productivity during production hours. Unplanned outages serve as effective indicators that this change process is being circumvented.
- Use change success rate as a key IT management performance indicator. Where changes are unmanaged, unmonitored, and uncontrolled, change success rates are typically less than 70 percent. Each failed change creates potential downtime, unplanned and emergency work, variance from plans, and business risk. Increasing the change success rate requires effective preventive, detective, and corrective controls.
- Use unplanned work as an indicator of effectiveness of IT management processes and controls. High performing IT organizations spend less than 5 percent of their time on unplanned work, while average organizations often spend 45 percent to 55 percent of their time on unplanned (and urgent) activities.

1.5 The Internal Auditor's Role

The audit committee wants to ensure that management has identified and assessed risks that could impede achievement of business objectives. Robust processes must be in place to mitigate, manage, accept, or transfer the risks effectively. Internal auditors serve as the eyes and ears of management and the audit committee, seeking out areas that require strengthening. To this end, the importance of an effective change management process cannot be underestimated, and internal auditors should consider conducting reviews of it on a regular basis.

This guide tackles IT change and patch management as a management tool, addressing:

- Why IT change and patch management are important.
- How IT change and patch management help control IT risks and costs.
- What works and what doesn't.
- How to know whether IT change and patch management are working.
- What internal auditing should do.

The guide's appendices offer tools for management and auditors to understand and address the risks inherent in IT change and patch management.

2.1 Why IT Change and Patch Management Are Important

Recent research has demonstrated that poor IT change and patch management increases downtime and costs. Prominent examples illustrate the problem. CNET News reported that in 2001, a "router configuration error" at Microsoft interrupted service to Microsoft.com, MSN.com, Expedia.com, and others. Full service was not restored until 22 hours later.¹ In 2004, the *Globe and Mail* reported on a relatively minor software change at Royal Bank of Canada that resulted in "10 million RBC customers who couldn't be sure of their account balances for days at a time and untold number of people left waiting for pay deposits and other transfers."² Where do you even begin to tally the costs of such problems?

Consider that organizations with better IT change and patch management:

- Spend less money and IT energy on unplanned work.
- Spend more money and IT energy on new work and achieving business goals.
- Experience less downtime.
- Install patches with minimum disruption.
- Focus more on improvements and less on "putting out fires."

If organizations need more incentive than this, Sarbanes-Oxley (for those that it affects) provides it by requiring executive management to understand and sign off on the controls over financial reporting, including IT controls. Without effective IT change management, it is difficult to see how management can meet the Act's requirements and affirm the integrity of financial statements.

2.2 How IT Change and Patch Management Help Control IT Risks and Costs

Any IT risk can be exacerbated by ineffective IT change management. Conversely, risks can be controlled by judicious, well-designed change and patch management processes. It may be less obvious that good IT change and patch management can reduce costs.

Without adequate control and visibility, an organization can spend money and effort on unneeded or low-priority changes while neglecting more important initiatives. Poorly designed or ill-considered changes can cause disruptions that must be addressed after the fact, or the changes must be "backed out." IT changes to one component can disrupt the operation of other components. These disruptions cost time and money, but they can be mitigated by good IT change and patch management processes.

Ultimately, inefficient or ineffective IT change management can cost an organization through:

- Attrition of highly-qualified IT staff due to frustration over low-quality results.
- Poor-quality systems that make employees ineffective and inefficient, or that alienate customers.
- Missed opportunities to provide innovative or more efficient products and services to customers.

Well-designed, rigorously-implemented IT change management processes can produce the opposite results. IT efforts can be focused on business priorities. Firefighting can be minimized. IT staff can be retained and motivated to excel. Employees can be provided with tools that boost their productivity. Customers can be pleased with systems that meet their needs.

2.3 What Works and What Doesn't

To be effective, IT change management must provide the organization's management with visibility into:

- What is being changed, why, and when.
- How efficiently and effectively changes are implemented.
- What problems are caused by changes, and how severe these problems are.
- How much the changes cost.
- What benefits the changes provide.

Such visibility is provided with metrics and indicators reported regularly and objectively. These are the dashboard gauges providing management with the necessary visibility.

IT change management provides the accelerator, break pedal, and steering wheel (and a reverse gear for returning to previous configurations) to control the IT vehicle through:

- Early and frequent involvement by management and end users to align IT changes with business needs.
- A defined, predictable, repeatable process with defined, predictable, repeatable results.
- Coordination and communication with constituents affected by changes.

2.4 How to Know Whether IT Change and Patch Management Is Working

As a rough guide, management (including IT management) can understand whether change and patch management are

¹ "Microsoft blames technicians for massive outage," CNET News, Jan. 24, 2001.

² "RBC blames human error," GLOBEANDMAIL.com, June 10, 2004.

working by asking some simple questions and scrutinizing the answers:

- Do we have an effective change management process?
Is the answer a denial of the importance of IT change management or an affirmation of its importance and acknowledgement of improvements underway?
- What controls are in place in our change management process?
Are controls in place and being improved or just being evaluated and deferred until fire-fighting subsides?
- Have we seen benefits from the change management process?
Are there measurable benefits, or is the emphasis on the costs of the IT change management process?
- Remember that site-wide outage we had last week because of a change? What happened?
How much does management know about what causes outages? How much control does management have over recurrence of the problem?
- What process was used to determine the cause of the outage?
Was it ad hoc or methodical? Did problem diagnosis quickly determine whether or not the outage was caused by a change, and if so, which change caused the problem?
- How does IT monitor the health of the process?
Are the indicators and measures objective and truly indicative or subjective and suspect?
- What is the goal of our change management process?
Is it focused on reliability, availability, and efficiency, or is it focused on other, less crucial goals? For that matter, is it focused at all?
- How disruptive is our patching process?
Is patch management part of a defined, repeatable change and release process, or is it ad hoc, informal, and emergency-based?

Recent research suggests that organizations with better IT change and patch management processes require fewer system administrators. When IT change and patch management work well, IT personnel are more effective and productive.

More rigorous, formal measures can and should be reported to provide maximum visibility into the effectiveness of IT change and patch management such as:

- Changes authorized per week.
- Changes implemented per week.
- Number of unauthorized changes that circumvent the change process.
- Change success rate (percentage of actual changes made that did not cause an outage, service impairment, or an episode of unplanned work).

- Number of emergency changes (including patches).
- Percentage of patches deployed in planned software releases.
- Percentage of time spent on unplanned work.
- Percentage of projects delivered later than planned.

2.5 What Internal Auditing Should Do

This Global Technology Audit Guide (GTAG) is about managing risks that are a growing concern to those involved in the governance process. Like information security, management of IT changes is a fundamental process that, if not done well, can cause damage to the entire enterprise. This enterprise-wide impact makes it of interest to many audit committees and, as a result, to top management.

This guide provides tools to help internal auditors obtain and evaluate evidence that IT management's assertions (performance, effectiveness, efficiency) are accurate. Mirroring the process of a financial audit³, IT auditors should obtain underlying authorization data (e.g., authorized change reports) and corroborating information (e.g., report of production changes from detective controls, reconciliations of production changes to authorized changes, system outages, etc.). By doing this, auditors can competently express an opinion on IT management's assertions of their change management processes and its ability to mitigate risk to the financial statements.

Internal auditing can assist management and the board of directors by taking the following actions:

- Understand the objectives of the organization regarding confidentiality, integrity, and availability of IT processing.
- Assist in identifying risks that could arise from changes and determining whether such risks are consistent with the organization's risk appetite and tolerances.
- Assist in deciding an appropriate portfolio of risk management responses.
- Look for and foster a culture of disciplined change management, including promoting the benefits of good change management.
- Understand the controls that are crucial to a solid IT change management approach.
 - Preventive.
 - Appropriate authorizations.
 - Separation of duties.
 - Supervision.
 - Detective.
 - Detection of unauthorized changes.
 - Monitoring of valid, objective change management metrics.
 - Corrective.
 - Post-implementation reviews.
 - Change information fed into early problem diagnosis steps.

³ Adapted from Montgomery's Auditing: 12th Edition, Chapter 1: "Overview of Auditing." [O'Reilly 98]

- Keep up-to-date on leading IT change and patch management processes and recommend that the organization adopt them.
- Demonstrate how management can reap the benefits of better risk management, greater effectiveness, and lower costs.
- Assist management in identifying practical, effective approaches to IT change management.

2.6 An Illuminating Dialogue Between a CIO and a CAE

One of the challenges for effective IT governance and auditing is asking good questions that reveal how IT managers think and verify that IT strategies and tactics are meeting business objectives. Often, discussions focus on the technologies rather than the management and control processes for implementing and sustaining the technology and operating the technology efficiently.

Change management is viewed by many as needless bureaucracy instead of an enabler for achieving business goals. Further, technologies such as patch management software systems are mistaken by many IT organizations as a substitute for a robust change management process. While change management software may automate controls to help ensure enforcement of the change management process, having the software alone does not provide the necessary results.

Senior audit executives can provide useful guidance and coaching to IT managers without going into technical details that divert attention from the real question: *Are our change management processes effective, and are we governing the right change-based IT activities?*

To show how quickly CAEs can ascertain the health of IT change management processes, we include a fictitious dialogue between Sydney, who has just started her tenure as a *Fortune* 500 CIO, and Jonah, a CAE. The dialogue shows how mistaken assumptions manifest themselves in even senior IT managers, and how those assumptions can be effectively challenged to cause dramatic changes in their belief systems and focus.

Why a dialogue? Dr. Eliyahu Goldratt gained prominence in the 1980s for his work on the Theory of Constraints, which is one of the three key management movements of this decade. (The other two management and problem solving systems are Total Quality Management by Dr. W. Edward Deming and manufacturing methodologies such as Just In Time). Dr. Goldratt may be most famous for his book *The Goal: A Process of Ongoing Improvement* [Goldratt 92], where the protagonist is a plant manager attempting to increase quality and decrease cost before his plant is shut down in 60 days. His book has sold millions of copies and is used in hundreds of university courses worldwide. This dialogue is inspired by *The Goal*.

2.6.1 Sydney's Belief in Her Patch Management Plan Shatters

Last week, Sydney was promoted from director of operations to CIO. She faces the challenges of dealing with not only all IT availability and cost competitiveness issues, but nagging security issues. Rumors are running rampant that her entire division is going to be outsourced.

Sydney is waiting to join the audit committee meeting. Waiting with her is Jonah, the CAE who joined the company six months ago from a well-known global telecommunications firm. She wonders whether she should take this opportunity to get acquainted with Jonah. Developing a mutually respectful working relationship with him could enhance her tenure as CIO.

Sydney first starts by admitting, "Jonah, I'm actually a little nervous about this meeting. This is my first update on the status of the company's information security program." Jonah is a veteran of numerous interactions with the audit committee, and he is immediately sympathetic.

"Oh don't worry. If you can articulate your goals clearly and describe what you need to do to achieve them, I'm sure you'll have no problem. Don't let the reputation of the audit committee get to you. I've been on both sides of the table, and I think these folks are the most professional I've met; competent and nice too."

"Really? I understand you joined us from ABC Telecom earlier this year. Were you in charge of internal audit there?" asks Sydney.

"No, my background actually includes some time in IT, as well as financial auditing and fraud investigation," replies Jonah. "Think of me as a business person who just happens to work in internal audit."

Hearing this, Sydney feels immediately relieved. We have similar backgrounds! "So you understand what I'm dealing with. That's a real relief! You can appreciate what I'm going through. We've really turned the corner on closing the holes in information security. I intend to tell them what we've been doing to apply patches more quickly to reduce vulnerabilities to worms and viruses. Before being appointed to CIO, I was in charge of developing our new patch management system."

Jonah looks skeptical. "You felt you needed a whole new system to help you manage patches?"

"Yes," replies Sydney. "We've been working on this for six months to address an audit issue and reduce our workload. It's really helped improve efficiency and security. We'll never miss an important patch again."

Jonah frowns. "Wow, you certainly don't hear that very often. Let me ask you this: when is it acceptable not to deploy a patch?"

Sydney is starting to frown a little now. Jonah seemed like a pretty smart guy, but he's sure asking some odd questions. She replies, "Well, never! Missing patches is exactly what earned us the audit finding in the first place. My goal is to make sure we always have patches deployed as quickly

as possible. After all, we have to make sure these servers are secure! Not only are we going to be more secure, but we'll be more efficient as well."

Jonah seems a bit exasperated. "Oh really? You're deploying patch management technology and actually seeing greater efficiency?"

"Absolutely. We've had some pretty great results. In fact, we just reached the 60 percent server coverage milestone."

"And you were able to increase efficiency ... by how much?" asks Jonah.

"Well, I don't have all the details, but I know the return on investment is significant." Digging through her briefcase, Sydney proudly shows Jonah the inch-thick report. "Here it is. By automating the patch process, we'll be saving between 300 and 600 staff-hours per month."

Jonah looks at the report but does not pick it up. "Amazing, 600 staff-hours monthly! That's more than three full time employees. Are you reducing head count by three people with all that saved labor?"

"Don't I wish! We always have a backlog of work because we're understaffed. There are always new projects, not to mention the constant break/fix fires that require us to drop whatever we were doing to repair the catastrophe of the day. That's precisely why we need to automate."

Jonah leans back and begins to smile as if she has confirmed some suspicion. Sydney starts to feel a little uncertain. He asks, "What are those two people who completed the rollout doing right now?"

"Well, as I said, they are dealing with issues ranging from operational fires and a few unforeseen challenges related to the new system. We invariably run into some patches that fail to apply correctly the first time and there are always some residual things we need to fix manually. These issues will be resolved once we get the process nailed down."

"So are you saying the initial success rate of the system is fairly low?" asks Jonah.

Sydney, feeling a little defensive, responds, "Well maybe, but I am certain we can turn it around with time."

Jonah asks, "Doesn't all of this unplanned work impact your availability?"

Uh, oh. Jonah mentioned availability. This is a definite sore spot. Sydney recalls the confrontational meetings with several business unit managers who were impacted by some failed patches. "Well, sure it has, to some extent. Where are you going with this?"

Jonah ignores her question. Instead, he asks, "And has this patch management system resolved your audit findings? My report to the audit committee today indicates the target completion date on your action plan keeps getting pushed out."

Several moments pass as Sydney tries to think of a response. In as confident a voice as she can muster she says, "Well no, those audit findings are not resolved yet, but we're very committed to making the system work."

2.6.2 Jonah Concludes on the Facts

"Sydney," Jonah starts, "I'm going to guess that if you haven't increased availability or security, and if you haven't decreased operational expense, and if you are actually generating more unplanned work, then you can't really tell me that you're increasing efficiency!"

"Furthermore, you are most certainly accelerating your rate of change by deploying patches without increasing your change success rate, so your amount of unplanned work must be going through the roof. I'm guessing that your business unit managers are so upset that they're screaming to get this entire system unplugged."

Stunned, Sydney wonders just what she has gotten herself into by starting a conversation with Jonah. She was going to proudly present her patch management plan and now she is not at all sure this is a good idea.

"Jonah, how can you know these things? I wish we had a little more time because you seem to have put your finger on some of my biggest problems."

"I feel the same way. If we had a little more time, I think I could help you keep the IT work within the company and save your new job."

"Now wait a minute! My organization is not in trouble. With software as crappy as it is these days, you have to automate the patch process to keep the infrastructure secure. The business keeps forcing insane demands on us with no understanding of IT or security."

"Sydney, it is clear to me that you are not running an efficient and secure IT operation; in fact, you're probably running a very inefficient and insecure operation. If the audit committee begins asking questions, this will become apparent, and they may feel you are not managing the risks properly. Just from this discussion, I believe there are some systemic IT change control issues here. I don't think you have the preventive, detective, and corrective controls you need to enforce adequate segregation of roles and effective supervisory controls."

"Are you saying that my people are lying to me?"

"In general, people rarely lie about these things. However, your measurements certainly are. When you talk about efficiency, you are missing the entire point. You need to think about it some more. I'm traveling during the next two weeks, but you can call my assistant to set up an appointment to talk about this if you'd like." With that, Jonah gets up and enters the conference room.

Sydney is later called into the meeting and successfully presents the information security plan and achievements to the audit committee. Within 15 minutes, she is excused and returns to her office.

"What in the world happened here?" she wonders. Before her conversation with Jonah, patch management was the center of her plan, and she was eager to use its success to show everyone how competent she was. But after her conversation with Jonah, her confidence was shaken to the core. So much so that she only briefly mentioned it in

her presentation to the audit committee. Worst of all, she can't figure out what is wrong.

Sydney admits to herself that her patch management system rollout is not going as planned. Her project completion date is advancing with each passing day. She wonders how Jonah could know that the project is beginning to go off-track. What did he mean by saying she was missing the point and wasn't managing properly?

The outcome of this dialogue is contained in Section 5, page 24.

Internal auditors and IT professionals have ample guidance on the disciplines of computer operational change management and change control. These processes have been well defined in publications going back to *Computer Control and Audit*, by Mair, Wood & Davis [Mair 73], and others. The Institute of Internal Auditors' landmark 1977 publication, *Systems Auditability and Control* was updated in 1994 and properly reflects the importance of this topic to management and internal auditors:

Change and problem management is critical to achieving a stable, reliable, and well-controlled operation. It involves problem tracking, escalation procedures, management review of problems and changes, prioritization of resources, controlled movement of programs into production, and systems software change control.

However, only recently have serious efforts been made to understand which IT practices and environmental conditions drive business results. New research published by the Software Engineering Institute and the IT Process Institute in 2004 shows that one of the key differences behind high- and low-performing IT and security organizations is the presence of an effective culture of change management. In other words, change management is not only a key foundational control, but also has potential benefits to the business.

The report, entitled *Best in Class Security and Operations Round Table Report* (BIC SORT) [Allen 04], captures some of the differences between high- and low-performing IT and security departments. The report describes their top issues and concerns, the resulting processes and procedures used to respond to these, as well as the belief systems and cultures that sustain these processes and procedures. With this insight, the authors learned how the high- and low-performing organizations behaved, both quantitatively and qualitatively.

In low-performing organizations, management cannot rely on IT change management to support the business adequately. Exacerbating this, where change management discipline is lacking, rigorous measurement and visibility are lacking as well. Management — and internal auditing, for that matter — have no reliable way to accurately assess the effectiveness and efficiency of the change management process. When the assurance of change controls supporting a business process is sufficiently undermined, assurance of the business process is also undermined. In contrast, high-performing IT change management organizations can provide accurate, focused information to fine-tune their own performance and to allow management and auditors to assess the change management process along with its ability to support affected business processes.

As internal auditors, we should become familiar with this type of information and apply it in audit reviews, to help our organizations manage our IT investment with greater efficiency and effectiveness.

3.1 Change Creates Risk: Why Patches Must Be Treated as Just Another Change

Auditors are aware of the tight relationship between change and risk. IT assets seem to be in a state of constant change. IT management must deal with:

- Regular changes (typically application, middleware, operating system, or network software and hardware upgrades scheduled for implementation).
- Patches (changes to repair defective code or other vulnerabilities discovered in production).
- Emergency changes needed to fix immediate issues causing service disruption.

Effective IT change management enables the organization to move safely from one known and defined state to another, regardless of the reason for making a change.

IT assets are easiest to manage and control when there is no pressure to implement or deliver change. For example, consider the virtuous characteristics associated with having change freeze periods: service levels and availability are highest, and the IT department is spending the majority of its time on planned work.

However, what happens when critical vulnerabilities are discovered and the level of urgency for change rises? What happens when numerous vendors with whom you do business are releasing patches regularly to repair critical flaws? According to PricewaterhouseCoopers [PWC 04], the sheer volume of changes is growing, which can have a significant impact on IT management's strategy for handling them:

Application and operating system software contain a large number of errors and vulnerabilities that continue to be discovered well beyond original release dates. In 1999, 417 software vulnerabilities were reported, according to the CERT® Coordination Center⁴ at Carnegie Mellon University. By 2003, the number of reported vulnerabilities had climbed to 3,784 — or about 73 [new] vulnerabilities every week.

In the BIC SORT workshop, many participants identified as a critical issue the volume of urgent patches to be applied to the operational infrastructure and the absence of an effective management process for handling these. However, the contrast between how the high- and low-performing organizations perceived and responded to this issue was remarkable. High-performing organizations patched their infrastructure far less often than low-performers. Even more illuminating was comparing the belief systems that guided IT management when they were making patching decisions.

In low-performing organizations, patch deployment is characterized as ad hoc, chaotic, and urgent. The availability of a patch to address a critical security vulnerability can be disruptive and often results in significant amounts of resources redirected from planned work to address the unplanned patch. Worse, even successful deploy-

⁴CERT® is registered in the U.S. Patent and Trademark Office by Carnegie Mellon University.

GTAG — Why Should I Care About the Way My Organization Is Managing Change? — 3

ment of the patch can cause unintended problems, such as servers becoming nonfunctional and thus unavailable to deliver critical services. A survey of U.S. federal chief information security officers (CISOs) conducted by Intelligent Decisions and reported by *InformationWeek* [Hulme 04] rated concerns about staying on top of patch management as their biggest problem:

Patch management ranked so high because it touches every part of their infrastructure, and there are so many patches coming out that everyone is worried whether or not they're keeping up.

In contrast, high-performing organizations treat a new patch as a predictable and planned change subject to the normal change management process. The patch is added to the “release engineering candidate” queue, where it is evaluated, tested, and integrated into an already scheduled release deployment. Following a well-defined process for integrating changes leads to a much higher change success rate. Interestingly, many high performers apply patches much less frequently than the low performers, sometimes by as much as one or two orders of magnitude. The high performers view the risk of the vulnerability exposure as less than the risk to availability due to unanticipated impacts of a bad or out-of-cycle change. Conversely, high-performing organizations that opt to deploy a patch as a high priority change are able to do so in a predictable, repeatable manner through the use of an effective change management process.

.....
High performers apply patches much less frequently than the low performers, sometimes by as much as one or two orders of magnitude!
.....

Given this insight and for the duration of this guide, we treat patches as a category or class of change, subject to the normal change management process. Two key implications emerge: patch management is a subordinate function to change management, and often, an effective change management process can help ensure the technologies used to address the “patch and pray” problem do not create additional problems.

3.2 We Already Have a Change Management Process — What Is Different Here?

One key aspect of effective management is that the organization has comprehensive, well-defined preventive, detective, and corrective controls in place, as well as clear definition and separation of roles. Change management controls enable management to address new requirements (such as new development projects and government regulations) without having to increase resources. Generally, effective change management mitigates risk, lowers cost, and provides resources for additional services.

Conversely, ineffective change management is a high risk. In most organizations, it is not a question of whether a change management process exists — it is whether the process is as effective and efficient as possible, and is used for all IT changes. In deploying emergency changes, it is extremely difficult to prevent errors, irregularities, and unintended disruptions. Disruptions to IT availability (resulting in low service quality and customer dissatisfaction) often drive organizations to consider and implement change management processes and controls. Research indicates that high-performing IT departments continually look for ways to improve their operational processes, including change management. By improving control and predictability for changes to systems and networks, your IT department can be on its way to becoming a best-in-class organization. Internal auditors are in the perfect position to help management improve these processes and controls.

.....
If the IT department can't describe all changes and their current states, it can't describe what is being managed or whether changes are happening as planned.
.....

Although easy to talk about, change management is one of the most difficult disciplines to implement. It requires collaboration among a cross-functional team of applications developers, IT operations staff, auditors, and business people whose focus is on end-to-end business services. It is important to note each group has a specific role to play, and these roles should be defined in change management procedures.⁵

Internal auditors are proficient at flowcharting business processes and assessing controls. They are in the best position to help their organizations see the benefits of looking at key processes from a global perspective.

The IT department must be able to assess and report the status of all changes at all times. Effective change management processes provide the information and assurance needed to keep track of all changes in their various states of completion.

Ultimately, the goals of better managing an organization's IT changes are to reduce risk (primarily associated with the inability to conduct business functions due to downtime), reduce unplanned work (thereby freeing up constrained resources), eliminate unintended results (caused by errors or omissions), and improve the quality of service for all internal and external customers.

3.3 How a Robust Change Management Process Can Help

Requests for change arise in response to a desire to obtain business benefits, such as reducing costs or improving services, or the need to correct problems. The goal of the

⁵ Sample roles are described in Appendix A, Table 4 (page 37). Additionally, an organization needs to ensure that the duties of the participants in the process are appropriately segregated (Table 5, page 37).

change management process is to sustain and improve organizational operations. This is accomplished by ensuring standardized methods and procedures are used for effective and efficient handling of all changes and minimizing the impact of change-related incidents on service quality and availability.

To protect the production environment, changes must be managed in a repeatable, defined, and predictable manner. Care must be taken to ensure changes made to correct one application, server, or network device do not introduce unintended problems on other devices or applications. This is especially important for IT assets (software, hardware, information) supporting the company's critical business processes and data repositories.

Strong change management processes can also assist the organization in maintaining ongoing compliance with new and expanding regulatory issues. Activities that address the potential impact of changes on regulatory compliance must be included within the risk management and business unit approval steps of the change process. For example, care must be taken when implementing changes to technology supporting the financial reporting process to ensure continued compliance with Sarbanes-Oxley. Likewise, changes in the handling of personally identifiable information in Europe can run afoul of European Union privacy directives.

Effective change management processes must be documented to reduce the ongoing effort needed to map, validate, and certify changes in the financial reporting process to support Sarbanes-Oxley compliance. In Section 404 of the Act, management is required to validate and assess controls over the financial reporting processes, including IT controls. Uncontrolled changes in the production environment can lead to errors that, if pervasive or critical, could be considered significant deficiencies that must be reported to the organization's audit committee. More serious deficiencies, called "material weaknesses" in the public accountant's world, are required to be disclosed publicly by companies through US Securities and Exchange Commission filings. Public disclosure of deficiencies could impact the organization's reputation, stock price, and ability to stay in business.

.....

Sarbanes-Oxley Section 404 requires that management validate IT controls. Uncontrolled changes in the production environment can lead to serious deficiencies and material weaknesses.

.....

In the guidance document, *A Framework for Evaluating Control Exceptions and Deficiencies* [BDO 04], deficiencies noted in general computer controls, such as change management, are to be evaluated in relation to their effect on application controls. Specifically, the IT general control (ITGC)

weakness is classified as a "material weakness" if one or more of the following exists:

- An application control weakness caused by, or related to, an ITGC weakness is rated as a material weakness.
- The pervasiveness and significance of an ITGC weakness leads to the conclusion that there is a material weakness in the organization's control environment.
- An ITGC weakness classified as a significant deficiency remains uncorrected after some reasonable period of time.

Last year, many organizations noted serious deficiencies associated with the change management of general IT controls surrounding a portion of their financial reporting environment. If this should remain uncorrected in the current year, they will be at risk. Internal auditors can assist management by identifying these issues and helping to ensure they are corrected in a timely manner.

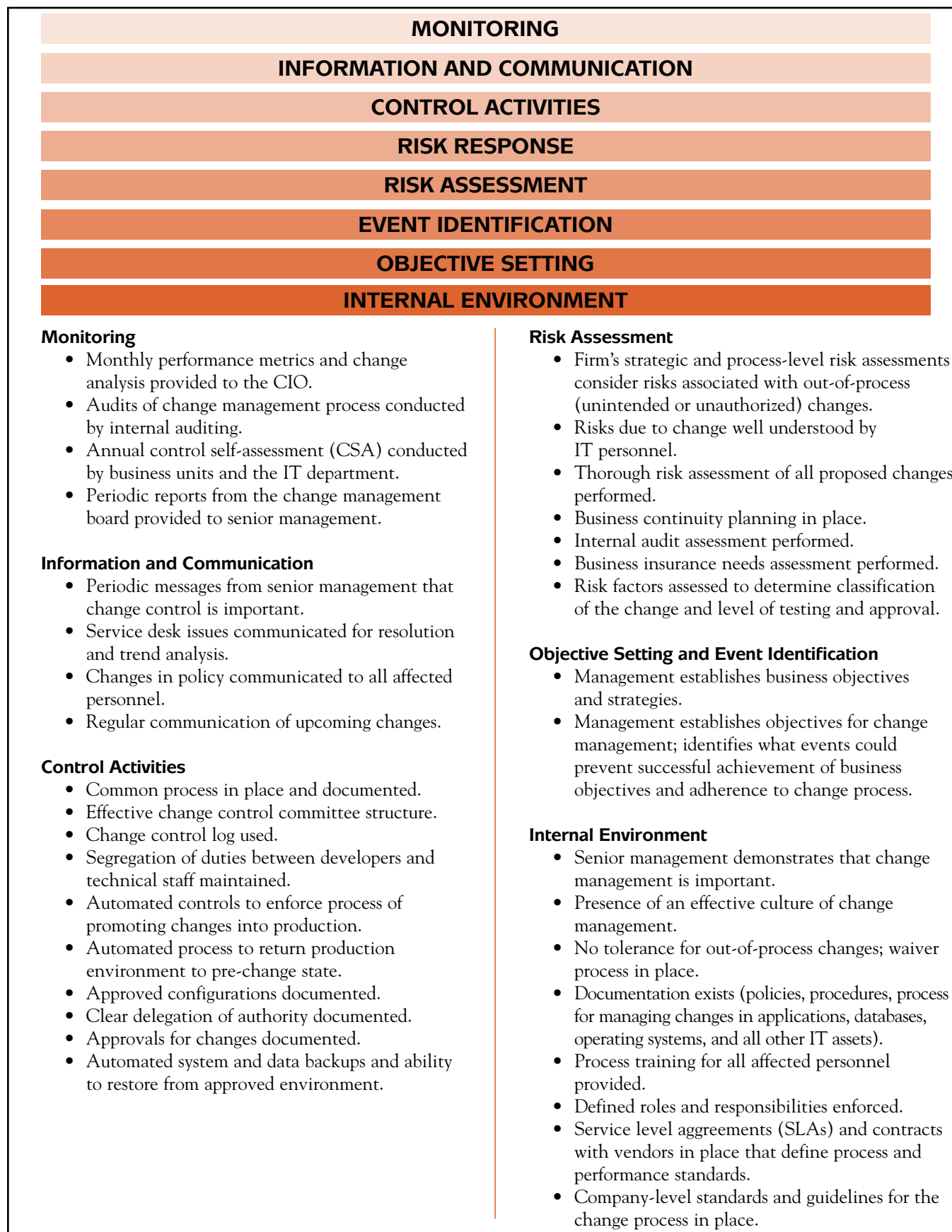
One model that is generally accepted for assessing internal controls is *Internal Control – Integrated Framework*, a model issued by The Committee of Sponsoring Organizations of The Treadway Commission – (COSO) in 1992. In 2004, this model was enhanced to provide an accepted enterprise risk management framework, which includes key principles, concepts, a common risk language, and clear guidance for implementation. This new direction, titled *Enterprise Risk Management – Integrated Framework* [COSO 04], provides four categories of organizational objectives and eight interrelated components of effective risk management. An illustration of how the COSO model may apply to change management is presented in Figure 1⁶ (page 12).

High performing organizations generally have a positive outlook on controls. As a case in point, effective change management processes reduce the risk of being a low performer and cause fewer issues to be highlighted by the external public accountant or equivalent regulator or review authority. As a result, the enterprise has a more satisfied Audit Committee and there is a companion reduction in pressure on IT department management. Typically a satisfied Audit Committee results in a much happier CEO, CFO, CIO, and CAE. Ultimately, organizations that treat change management controls as enablers for effective business conduct are more successful. The key point to remember is that change management centers on process with a managerial and human focus, and is supported with technical and automated controls.

⁶ Derived from COSO's "Enterprise Risk Management-Integrated Framework," September 2004. An executive summary is available at http://www.coso.org/publications/erm/coso_erm_executivesummary.pdf.

GTAG — Why Should I Care About the Way My Organization Is Managing Change? — 3

Figure 1: COSO ERM Model for Change Management



In most companies, the IT department has two primary roles: 1) operate and maintain existing services and commitments, and 2) deliver new products and/or services to help the business achieve its objectives. This section describes the scope of change management in support of these two roles, the characteristics of effective and ineffective change management, auditing's role in change management, and metrics that can assist in managing change effectively.

4.1 What Is the Scope of Change Management?

This guide focuses on IT operational change management, beginning when upgrades or updates to IT assets (infrastructure, applications) are identified for movement to production (e.g., from either an application development or research and development (R&D) team) and ending when such assets are retired from the production environment. This includes application maintenance and emergency change controls. Specifically excluded are the changes that occur during software design and development.

The term, *change management*, as used in the guide, excludes the process of configuration management. Configuration management is concerned with identifying, controlling, maintaining, and verifying the versions of all IT components (hardware, software, associated documentation) [ITIL 00]. However, the change management process must interact with the configuration management process (and companion controls) when changes are made to configurations.

4.1.1 Sources of Change

Virtually every business decision requires change in IT. The following factors serve as sources of change that must be addressed and managed effectively in the IT environment:

- External environment (competitive market, stakeholders/shareholders, changing risks).
- Regulatory environment.
- Business objectives, goals, strategies, requirements, processes, and shifts in priorities.
- Vendors (new products, upgrades, patches, and vulnerabilities).
- Partners and suppliers.
- Results of an audit, risk assessment, and other type of evaluation or assessment.
- Operational problems.
- Changes in performance or capacity requirements.

4.1.2 Scope of Changes

An effective change management process encompasses within its scope any and all alterations to any and all IT-based assets on which business services depend. Assets subject to change management include:

- Hardware: mainframes, servers, workstations, routers, switches, and mobile devices.
- Software: operating systems and applications.

- Information, data, and data structures: files and databases.
- Security controls: anti-virus software, firewalls, and intrusion protection/detection systems.
- Processes, policies, and procedures.
- Roles/responsibilities: authorization, authority to act, and access controls.

4.1.3 Change Management Process

A change management process typically includes the following activities:

- Identify the need for the change.
- Prepare for the change.
 - Document in detail the change request.
 - Document the change test plan.
 - Document a change rollback plan, in case of change failure.
 - Write a step-by-step procedure that incorporates the change, the test plan, and the rollback plan.
 - Submit the change procedure in the form of a change request.
- Develop the business justification and obtain approvals.
 - Assess the impact, cost, and benefits associated with the change request.
 - Review and assess the risks and impacts of the change request, including regulatory impacts.
- Authorize the change request.
 - Authorize, reject, or request additional information on the change request.
 - Prioritize the change request with respect to others that are pending.
- Schedule, coordinate, and implement the change.
 - Schedule and assign a change implementer.
 - Schedule and assign a change tester.
 - Test the change in a pre-production environment.
 - Communicate the change to stakeholders likely to be affected.
 - Approve the change for implementation.
 - Implement the change as requested.
- Verify and review the implemented change (a critical step that is most often overlooked).
 - Was the change successful?
 - Was the change process followed?
 - What was the variance between the planned and implemented change?
 - Were internal control, operations, and regulatory compliance requirements maintained?
 - What were the lessons learned that can be used to improve the process?
- Back out the change if unsuccessful.
- Close the change request and communicate with the affected parties.
- Make agreed-to changes to the change management process.

Auditors immediately will recognize that effective change management requires preventive, detective, and corrective controls, and that the need for independent controls increases as the IT production environment becomes more dynamic and complex. Necessary preventive controls include separation of roles, change authorization, as well as supervision and enforcement. However in order to monitor and enforce the process effectively, detective controls must be in place to monitor the production environment for changes, reconcile these changes to approved changes, and report any unauthorized variance. Effective change management also serves a corrective role for IT management during outages and service impairments, allowing change to be ruled out first in the repair cycle, thus reducing repair time.

4.2 What Does Ineffective Change Management Look Like?

How do you know if an organization has an effective or ineffective change management process? What behaviors and other signs serve as useful indicators of the organization's capability — or lack thereof?

Indicators of ineffective or absent change management appear as dysfunction in a range of organizational dimensions.

At the market level:

- Lost opportunities. The enterprise is unable to deploy planned, new products and services consistently. This occurs when having to commit resources to unplanned work, as a consequence of unmanaged changes. Unplanned work can be manifest as lost/unbudgeted-time, lost/unbudgeted resources (people, capital), and unbudgeted work.
- Development projects are late and often over budget, resulting in late and more costly products and services when compared with competitors.

At the client/customer/stakeholder level:

- Products and services do not perform as advertised or as intended, or operate with flaws. This leads to low, unreliable product or service quality. If customers can easily switch to another provider, they will.

At the organizational level:

- Unauthorized, untracked changes create potential exposure for fraud.
- Business requirements can be misinterpreted with respect to required IT changes and thus poorly or inadequately implemented.
- There is little to no ability to forecast the impact of a change on existing business processes.
- Given that changes are not likely to be evaluated with respect to one another, there is a lack of change prioritization, resulting in either working on the wrong things or working on something that is less important. The work may be done out of the intended sequence, resulting in rework and duplication of effort.

- A high degree of thrashing is evident, reflected in an attitude that “things just keep happening to us,” or “lots of energy is lost in the system,” and there is no ability to control the operational environment.
- Patching systems causes large disruptions due to failed changes, resulting in outages, service impairment, rework, or unplanned work. This often exacerbates a poor or adversarial working relationship between information security and IT operations.
- Large numbers of cycles (time, resources, capital) are spent on correcting unauthorized project activities or infrastructure, taking cycles away from planned and authorized activities.
- Resources regularly are diverted to rework, as a result of having to address the unintended consequences of unmanaged changes.
- There is high turnover in technical staff and evidence of “burnout” in key staff.

At the IT infrastructure level:

- Ad hoc, chaotic, urgent behavior requires regular intervention of technical experts/heroes; a high percentage of time is spent in “firefighting” mode on reactive tasks.
- An inability to track changes, report on change status and costs, and the presence of unauthorized changes.
- Increasing resources spent tackling unplanned work at the expense of planned work. This can be described as a low change success rate. Change success rate is a measure of the amount of new work introduced when a change is implemented. A high change success rate means the change is implemented as planned, and no additional work is introduced as a result of the change. Conversely, a low change success rate means a change unexpectedly introduces additional unplanned work, sometimes in excess of the work required to implement the original change. A low change success rate can produce a downward spiral that continues to consume excessive resources.
- Ineffective IT interfaces with peers (R&D, application developers, auditing, security, operations) that create barriers and introduce unnecessary delays.
- Numerous undocumented changes happening over time increases configuration production variance, causing lower change success rates and increasing the difficulty of deploying patches without failed changes and unplanned work.

4.3 What Does Effective Change Management Look Like?

How do you know effective change management when you see it? Can you walk into an organization and determine within 15 minutes if it has an effective change management process?

Indicators of effective change management appear as mature capability (predictable, repeatable, managed, measurable, measured) in a range of organizational dimensions.

At the market level:

- The enterprise is positioned to act on new business opportunities that require additional or upgraded IT capability. Each opportunity is planned and managed in a predictable manner. Adequate resources can be committed with the confidence that they are sufficient, and based on tracked, historical performance.
- IT-supported products and services are released to the market as planned and expected.

At the client/customer/stakeholder level:

- Products and services perform as advertised and demonstrate a consistent, reliable level of product and service quality. Customer issues and complaints are dealt with in a timely manner. Customers are generally satisfied and loyal to the organization.
- There is a decreasing demand for customer support center/help desk resources.
- Appropriate stakeholders are involved in assessing risks associated with proposed changes and prioritizing their implementation.
- Participants in the change process understand the relevant categories and priorities of changes and the levels of formality and rigor required to implement each of these.
- A posture of compliance, because of the foundational nature of change management. Virtually every regulation has IT requirements and, as a result, can create a new project for compliance and security teams. When controls are well documented, complying with a new regulation is not a new project, but merely a mapping activity.

At the enterprise level:

- A culture of change management is evidenced by understanding, awareness, visible sponsorship, and action.
- Effective tradeoffs are performed regularly, balancing the risk and cost of change with the opportunity. Changes are scheduled and prioritized accordingly. There is an ability to forecast the impact of the change on the business. According to BITS [BITS 04]:

Determining the risk appetite of a company is often the most difficult step in implementing a patch management strategy. Individuals who are responsible for the patch management process should understand their organization's risk tolerance with respect to installing patches and help to identify and distribute patches in the organization, using the organization's severity rating as a guide.

- Resources (time, effort, dollars, capital) are applied to implement selected changes, with little to no wasted effort (high change success rate); resources rarely are diverted to unplanned work.

- The organization can confidently answer the questions: "Am I doing the right things?" (an ability to select and prioritize) and "Am I doing things right?" (with acceptable quality and performance).
- An effective change management process is evidenced by rigorous process discipline and adherence/enforcement, centralized decision-making authority, and cross-departmental communication and collaboration.
- Authorized projects are mapped to work orders and vice versa.
- Compliance and security investments are sustained because production configurations do not drift into noncompliant or nonsecure states. Consequently, the cost of security and compliance are much lower.
- Increasingly, more time and resources are devoted to strategic IT issues, due to the organization having mastered tactical (day-to-day operational) concerns.
- Effective change management serves as an essential control for IT governance.

At the IT infrastructure level:

- Change management controls (embedded in well-defined IT operational processes) are used to help ensure the consistency and predictability necessary to achieve business goals that rely on these processes. In other words, IT staff understands how effective change management supports meeting business objectives.
- A culture of change management is perpetuated by a combination of tone at the top and preventive, detective, and corrective controls, which serve to deter future unauthorized changes. Management explicitly states that the only acceptable number of unauthorized change is "zero."
- A high change success rate is present, resulting in the absence of, or at least minimal, unplanned work. The absence of urgency and a well-defined process for integrating changes lead to a much higher change success rate.
- Effective change controls are in place, regularly reported, and easily audited. Preventive controls are well documented and consistently executed, and detective controls are used to supervise, monitor, and reconcile changes to authorized change orders. Controls are conducive to substantive sampling by auditors, requiring little to no additional information from IT management.
- Variances in production configurations are detected early so as to incur the lowest cost and least impact.
- The enterprise regularly demonstrates operational excellence with respect to change management.
- Higher service levels (high availability/uptime/mean time between failures, low mean time to detect problems/incidents, low mean time to repair) occur in the presence of well-defined processes that introduce planned, predictable change.

GTAG — Defining IT Change Management — 4

- IT is able to return to a known, reliable, trusted operational state quickly when problems arise with a new change or configuration.
- IT demonstrates unusually efficient cost structures (server-to-system administrator ratios of 100:1 or greater, compared with at least one order of magnitude less in low-performing organizations).
- Timely identification and resolution of operational problems, including security incidents.
- Organizations with effective change management processes and controls tackle patches in a planned, predictable manner, subject to the same analysis and process as any other changes. Critical patches are added to the release engineering candidate queue, where they are evaluated, tested, and integrated into an already scheduled release deployment.
- Preventive and detective controls are automated, allowing for easier and more accurate reporting to auditors, requiring fewer manual inspections and substantive sampling resembling “archaeology.”
- Most effective organizations apply patches less frequently than the norm, perhaps by one order of magnitude, accepting the risk of the vulnerability exposure as less than the risk to availability due to unanticipated impacts of a bad or out-of-cycle change. However, in the event of a critical update, capable

organizations are able to implement an out-of-cycle patch with minimal risk.

To have an effective process, stakeholders are not just involved in assessing risks associated with proposed changes and prioritizing change implementation. One of the barriers that IT departments often face when trying to roll out a robust change management process is the lack of interest, involvement, and sponsorship from their business counterparts. Business unit managers should be actively involved in the entire process, from initial identification of their needs through conducting the majority of user acceptance testing and approving the changes being moved into production. These critical touch points are more likely to occur when the business manager’s role is included in relevant policies and procedures and senior managers place the appropriate emphasis on being co-owners in the process rather than observers. Communication and collaboration between IT and the business units is critical for an effective process.

4.4 Change Management Metrics and Indicators

Internal auditors should determine whether these key change management metrics are being used to monitor process effectiveness and drive business value. The metrics listed in Table 1 are useful indicators of an effective change management process.

Table 1: Change Management Metrics⁷

Metric and Indicators	Guidelines
Number of changes authorized per week, as measured by the change management log of authorized changes.	In general, more changes indicate more change productivity, as long as the change success rate remains high. The trend (up, down or steady) should make sense in the business context. High-performing organizations can sustain over 1,000 successful changes per week. ⁸
Number of actual changes made per week, as measured by detective controls such as monitoring software.	The number of changes actually implemented for the week should not exceed the number of authorized changes.
Number of unauthorized changes. These are changes that circumvented the change process. This is measured by taking the number of actual changes made and subtracting the number of authorized changes. Where detective controls are not present, no reliable measurement of actual changes can be made. In this case, the number of unplanned outages can be used as a substitute measure.	Lower is better, but typically the only acceptable number of unauthorized change is zero; one rogue change can kill an entire operation or create material risk. Large numbers of unauthorized changes indicate that “the real way to make changes” is to circumvent the change management process. High-performing organizations have a culture of change management and consequently state that they do not tolerate any unauthorized changes [Kim 03].

⁷ Further definitions of these metrics and indicators can be found in Appendix A, page 31.

⁸ Benchmarking done by the IT Process Institute.

Table 1: Change Management Metrics (cont'd)

Change success rate, defined as successfully implemented changes (those that did not cause an outage, service impairment, or an episode of unplanned work) as a percentage of actual changes made.	<p>Higher is better. When changes are not managed and not adequately tested, change success rates typically are around 70 percent.</p> <p>High-performing organizations not only regularly achieve change success rates of 99 percent, but failed changes rarely cause service interruptions or unplanned work.</p>
Number of emergency changes (including patches), determined by counting the number of changes that required an urgent approval during the week using the change review board or emergency change process.	<p>Lower is typically better. Many emergency changes indicate that the “real way to make changes” is to use the emergency change process either for convenience or speed.</p> <p>Emergency changes typically have a higher failure rate and generate unplanned work or rework. An increase in emergency changes may indicate that there are other change management problems causing this increase.</p> <p>ITPI benchmarking found that when emergency changes comprise more than 10 percent of total changes, the organization is almost certainly a low performer. In particular, two organizations that had catastrophic “front page news” IT failures were typically expediting more than 25 percent of their change requests.</p>
Percentage of patches deployed in planned software releases. When patches are deployed in planned software releases, they do not cause production disruption and have much higher change success rates.	<p>Higher is typically better.</p> <p>Paradoxically, high-performing IT organizations often have the lowest rate of patching. During the BIC SORT, two of the high performers stated that they choose to patch annually, despite making thousands of changes per week. They often mitigate vulnerability risks without requiring changes to production systems (e.g., blocking the vulnerability at a firewall).</p>
Percentage of time spent on unplanned work. Planned work is time spent on authorized projects and tasks. Unplanned work includes break/fix cycles, rework, and emergency changes.	<p>Lower is better.</p> <p>In the 11 high performing IT organizations the ITPI studied, all were spending less than 5 percent of their time on unplanned work. In contrast, hundreds of other organizations were spending 30 percent to 40 percent of their time on unplanned work.</p>
Percentage of projects delivered later than planned.	<p>Lower is typically better. When organizations are spending all their time on unplanned work, often there is not enough time to spend on planned work such as new projects and services, thus causing project results to be delivered late.</p>

GTAG — Defining IT Change Management — 4

Figure 2: Unplanned Work as Indicator of Effective Change Management Process

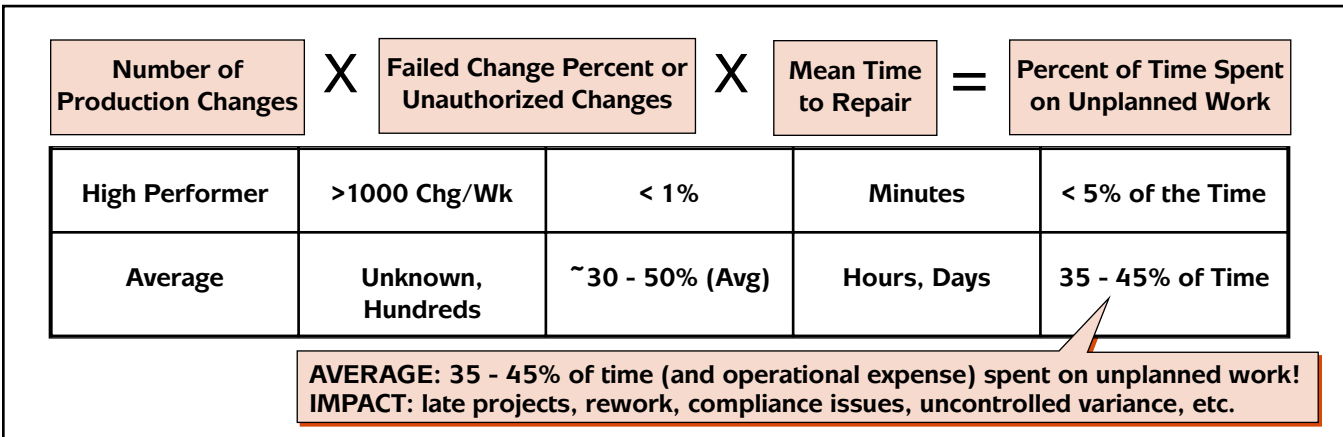
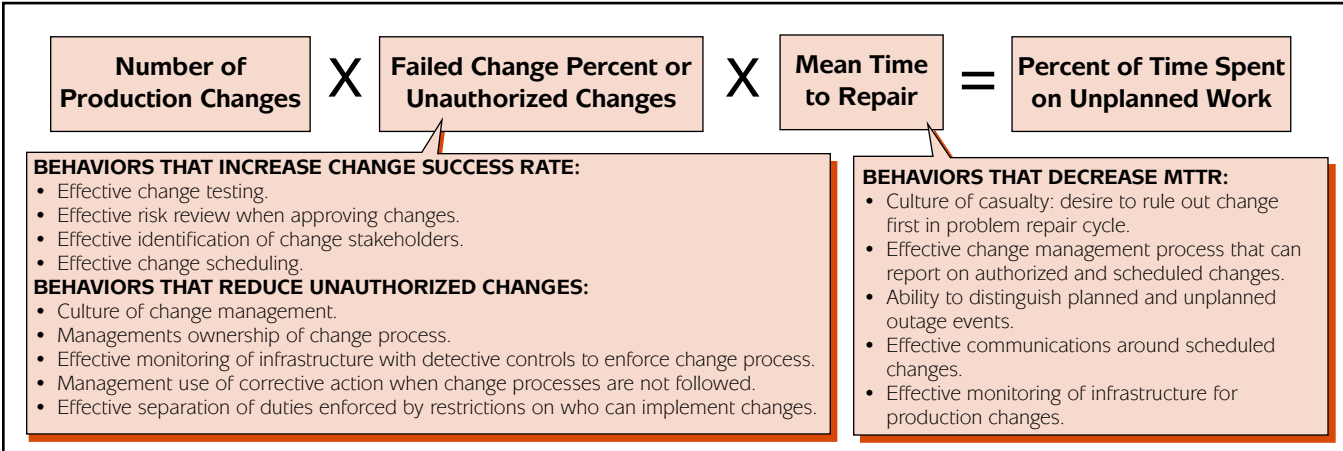


Figure 3: Key Variables That Influence Change Management Processes



Figures 2 and 3 show the key indicators of effective change management and the dominant controls that raise and lower them. The key indicators⁹ are:

- Number of production changes.
- Percentage of those changes that fail or are unauthorized.
- The amount of time required to recover the failed change.

When these three variables are multiplied together, the result is unplanned work.

This is an extremely simple model and is not intended to be mathematically correct. It is intended to show the dominant variables and leading indicators for effective IT change management, and consequently effective IT:

- When an IT organization makes no changes or is in a change freeze period, availability is at its highest and unplanned work is at its lowest.
- When an IT organization is not enforcing change management policies (i.e., inadequate preventive and detective controls), unauthorized and failed changes cause protracted outages, driving up unplanned work.

- When IT organizations have a high ratio of unplanned to planned work, they have less time available to do the work that they were tasked to do, such as delivering new products and services.

High-performing IT organizations will do even better than this model suggests. When changes are managed properly, even failed planned changes rarely cause an outage and consequently have a “zero” mean time to repair. On the other hand, low-performing organizations often cannot measure anything except the obvious outages and unplanned work.

4.5 Integrating Patch Management Into Change Management

Despite the urgency attached to applying software patches, patch deployment ideally belongs in pre-production processes, where the patches can be tested adequately in a staging environment. Ideally these patches are deployed as part of a scheduled software release.

Patching is often a risky operation for many reasons. Patches tend to effect many critical systems libraries and

⁹ Based on ITPI benchmarking that studied 11 high-performing IT organizations and surveyed hundreds of others.

other software used by many application programs. Patches tend to be large changes, often with little documentation describing what they change. Patches tend to be large and complex operations. Even small configuration variances can cause drastically different results. These factors make the change success rate for patches much lower than typical changes, thus requiring more comprehensive testing. When sufficient patch testing and planning is not done, the “patch and pray dilemma” invariably appears.

The “patch and pray” phenomenon is well-documented; it refers to the fact that neither patching nor avoiding patching seem to achieve the objective of creating an available and secure computing platform. As described above, high-performing IT organizations patch far less frequently than typical IT organizations, and yet they still achieve their desired security posture. It is incorrect to assume that they do this at the expense of security. Rather, they effectively manage residual risk and use compensating controls instead of patching.

Examples of how requests to patch production systems should be evaluated include addressing the following questions [ITPI 04]:

- Is this a material threat to our ability to deliver safe and reliable service to the business?
- Can we mitigate this threat without applying the patch or update?
- Can we test the impact of the update and feel confident that our tests will predict the outcome on our production systems?
- When is the next release cycle? Can we package this update with other tested updates?
- If we have to do this now, how can we minimize the risk of unexpected consequences?
- If we cannot reduce the risk of exposure through testing, and we cannot bundle this with any other releases, then can we get the stakeholders and IT management to sign off on the risk?

Create a release schedule that achieves the above objectives, attempting to bundle patches and updates into releases instead of applying individual patches to individual systems.

Many of these metrics are also identified in work completed in November 2004 by the Corporate Information Security Working Group’s, Best Practices and Metrics Team. This work was chartered by the U.S. House of Representatives Government Reform Committee, Subcommittee on Technology, Information Policy, and Intergovernmental Relations and the Census.¹⁰

Finally, the risks associated with change are not restricted to just applying patches, but can be generalized to any automated change deployment technology. John Gall succinctly wrote about the challenge of automation: “The

advent of the computer revolution merely provides new opportunities for errors at levels of complexity and grandiosity not previously attainable.” [Gall 86]

The use of patch management and change deployment technologies simultaneously make the IT production environment more dynamic and complex: the number of change vectors increases, as well as the number of changes that can be made. These environments require: 1) additional preventive controls to reduce the likelihood of unauthorized changes, and 2) independent detective controls to simplify the monitoring, reconciliation, and reporting functions.

4.6 Guiding Principles: How to Decide if, When, and How to Implement Changes

The guiding principles of how to make good change management decisions involve asking the following questions:

- Does the change really need to be made? IT organizations have the least amount of unplanned work and firefighting in change freeze periods. Consequently, any change must warrant not only the change preparation and implementation efforts, but the (often unforeseen) consequences of making the change.
- Are scheduled maintenance and change freeze periods, when no changes are allowed, defined? Periods of operational stasis are not only the most stable, but also the most productive, and therefore must be defined and enforced.
- If changes do need to be made, how do you ensure that the change will be successful? Untested changes rarely have a change success rate higher than 70 percent. Organizations committed to implementing successful changes must invest time and resources for adequate change testing.
- When changes must be implemented, are they scheduled in large batches? Variance creates risk, and variance can be reduced by packaging multiple changes so they can be tested and implemented simultaneously. This results in longer periods of preserved operational stasis as well as shorter and more productive change implementation times.
- Are variances being reported regularly to IT management? Are production changes being reconciled with authorized work? Are unplanned outages and change variances documented and acted upon? Are reports showing the effect of preventive and detective controls easily accessible to management and auditors? When controls are functioning properly, not only is the change audit process more efficient, but IT management is more likely to achieve its business objectives.

¹⁰ Information on this effort is available at <http://reform.house.gov/TIPRC/News/DocumentSingle.aspx?DocumentID=3030>. The Group’s November 2004 report is available at <http://www.educause.edu/LibraryDetailPage/666&ID=CSD3661>.

GTAG — What Questions Should I Ask About Change and Patch Management? — 5

In this section, we offer a set of questions auditors may use to get a sense of how effectively changes are managed. The goal of this section is to provide good questions and guidance on how to interpret typical answers given by several archetypes of IT managers with different views on the importance of effective change management.

The archetypes most commonly found are:

- IT manager with an effective change management process.
- IT manager with an ineffective change management process, but working on improvement (in problem solving mode).
- IT manager with an ineffective change management process and no plans to change this (in denial).

Table 2: Questions to Ask About Change Management by Archetype

Question to IT Manager	IT Manager With Effective Change Management	IT Manager in Problem-solving Mode	IT Manager in Potential Denial
"Change management is very important. Do you think we have an effective change management process?"	"Ours is world class. We're even ready for Sarbanes-Oxley Section 404 requirements because all of the controls are already in place. We have had to generate a few more reports to show the control mappings, but we're in good shape."	"Funny you should ask — we're working on this, but so is everyone else that is subject to Sarbanes-Oxley Section 404. We'll know more once we are further along."	"We have a process that seems to work. I haven't heard anything negative about our change management process, especially not from auditing. We can't afford the overhead of a burdensome process to fix something that's already working."
"What are your acceptable numbers of unauthorized changes?"	"The only acceptable number of unauthorized changes is zero. One rogue change can kill our entire operation, and that's why we reconcile changes daily. We trust, but verify."	"Well, when you ask it that way, of course the only acceptable number of unauthorized changes is zero. But would we bet our quarterly bonuses on it? No way. Especially after last quarter."	"Look, we don't get paid to not make changes. Sometimes we need to break the rules. That's how we really get work done here. Change management is bureaucratic, and they just want to slow things down."
"Describe what controls you need in your change management process."	"We require the preventive, detective, and corrective controls necessary to provide management with an accurate view of the work being done. We have defined some new change metrics and have identified a few more stakeholders that we need to involve in our change management committee. We had no idea that the bean counters actually cared about change management, so they will now be attending the meetings."	"We have an entire team of internal auditors and consultants working on a Sarbanes-Oxley-related project. They are defining and creating a plan to test specific controls. This whole Sarbanes-Oxley project revealed a need for integrated oversight and an enterprise view of change. We also uncovered some business processes that need to have better change control, and we're working on that, too."	"We're still in the analysis phase. We're just so busy with urgent business, and all we've had time for are the Sarbanes-Oxley-related controls. But we know it's important, and we will get to it as soon as we can. Besides, currently, we don't have any budget for this work. My experience tells me that what we have is probably good enough, because no one has told me specifically that the current process is inadequate."

GTAG — What Questions Should I Ask About Change and Patch Management? — 5

Table 2: Questions to Ask About Change Management by Archetype (cont'd)

Question to IT Manager	IT Manager With Effective Change Management	IT Manager in Problem-solving Mode	IT Manager in Potential Denial
"Have we seen benefits from the change management process?"	"Absolutely. In fact, the benefits have been so obvious that we have created an internal culture of change management. We no longer feel like professional fire-fighters. We have substantially improved our performance, uptime, and satisfaction, from our business customers, to our internal staff, and all the way up to the company executives."	"Yes, but we still are not where we want to be. We have reduced the amount of outages, and we have increased our change success rate significantly. Now, changes are happening inside the maintenance windows, although we still have the occasional 'cowboy' who forgets to go through the process."	"The pace of business is so high right now that we just don't have time to go through a cumbersome change management process that slows things down, lowers productivity, and creates a bureaucratic atmosphere. I don't always hold people accountable for following the change process, because they already are stretched so thin keeping the place running. But outages due to change do happen occasionally, and we know that we can't keep crashing the order management system."
"You remember that site-wide outage we had last week because of a change? What happened?"	"We determined the particular change that caused that 10 minute outage was authorized. However, we failed to anticipate the downstream effect on an unrelated system. But, this won't happen again."	"We found that a developer migrated a change outside of our agreed-upon process. He never should have been given approval authority for changes to that particular system. We fixed this in a hurry, and this developer can no longer even log onto the production servers."	"We found that one of our vendors was doing some maintenance and updated some software. Trouble is they overwrote a library that we had customized. They are supposed to keep track of our customizations so this was a violation of our maintenance contract."
"When you were working the outage, what was the process you used to figure out what went wrong?"	"The first thing we always do is rule out authorized changes as early as possible in the repair cycle. We knew immediately that the outage wasn't due to a scheduled change. Next, we checked for any emergency production changes. We found four changes that were made two minutes before the outage and then found out who made them. They did a change rollback, and we were up and running within minutes."	"We had a gut feeling that the problem was not coming from an authorized change. We test and deploy our changes only inside of specified release windows. So we started investigating, looking at logs, working backward from the outage, looking for anything outside of the release window. We eventually found out who made the change, but not why the change was made. I think that administrator learned a valuable lesson that day."	"Because we don't have a centralized process, several separate teams mobilized to try to figure out what was going wrong. We finally set up a SWAT team. They quickly figured out the outage was due to the vendor upgrade, but we had to conference them in to pinpoint that the cause was our library. They had no way to change the library back to the old version, so we had to restore the whole software directory from tape."

GTAG — What Questions Should I Ask About Change and Patch Management? — 5

Table 2: Questions to Ask About Change Management by Archetype (cont'd)

Question to IT Manager	IT Manager With Effective Change Management	IT Manager in Problem-solving Mode	IT Manager in Potential Denial
"How do you keep overall watch on the health of the process?"	"Change rate, change success rate, mean time to repair (MTTR), mean time between failures (MTBF), a count of unauthorized changes that circumvent process. We also have a coverage metric to show which parts of the enterprise are not participating in the process. Unplanned work is a great indicator. We always look for variance and try to figure out how to reduce it at the source."	"We measure how quickly we can implement a change. We measure mean time from change request to change closure. We're gearing up to measure change success rate as well as emergency and unplanned changes."	"We don't use fancy metrics, although we do insist on process excellence. I know we have lots of fires to fight, but you would too if you had to work with some of these people."
"What is the goal of your change management process?"	"Reliability, availability, and the reduction of cost. Two measures must go up while the third must go down. Trying to optimize just one of the three will put us out of business."	"We want to make as many changes as the business requires. We want to do them quickly and accurately."	"Our goal is to get attendance of all the key stakeholders in our change management meetings and be sure everyone is aware of what is going on and why. We figure as long as our audits are favorable, we're doing fine."
"How disruptive is your patching process?"	"Not disruptive at all. We understand that business availability is paramount. We have to figure out how to mitigate the security risks without all the dangers associated with changes. We average one big patch bundle per year."	"Patching used to be very disruptive, but after the big outage six months ago, we revisited every assumption we were making about which patches to deploy and when to roll them out. We have reduced the amount of time spent on patching from weekly to monthly, and are working on quarterly."	"Because of the poor quality of the software being released by vendors, we continue to spend too much time patching. It's a no-win situation. If we don't patch, our systems will be hacked. If we patch them, we risk crashing production systems. But, since we can't be plastered on the newspaper front page, we have no choice but to patch."

GTAG — What Questions Should I Ask About Change and Patch Management? — 5

5.1 Evolving a Change Management Capability

The management of change is an evolutionary process. Groups should not become discouraged as they start developing their change management processes. The solutions may require changing people, processes, and technology. The following illustrates typical stages of change management:

1. Oblivious to Change: “Hey, did the switch just reboot?”
2. Aware of Change: “Hey, who just rebooted the switch?”
3. Announcing Change: “Hey, I’m rebooting the switch. Let me know if that will cause a problem.”

4. Authorizing Change: “Hey, I need to reboot the switch. Who needs to authorize this?”
5. Scheduling Change: “When is the next maintenance window? I’d like to reboot the switch then.”
6. Verifying Change: “Looking at the fault manager logs, I can see that the switch rebooted as scheduled.”
7. Managing Change: “Let’s schedule the switch reboot to week 45 so we can do the maintenance upgrade and reboot at the same time.”

Figure 4 depicts a progression of change management capability from reactive to continuously improving.

Figure 4: Change Management Capability Levels

CHANGES CONTROL THE ORGANIZATION		ORGANIZATION CONTROLS THE CHANGES		
EFFECTIVENESS	REACTIVE <ul style="list-style-type: none">• Over 50 percent of time spent on unplanned work.• Chaotic environment, lots of fire fighting.• MTTR is very long; poor service levels.• Can only scale by throwing people at problem.	USING THE HONOR SYSTEM <ul style="list-style-type: none">• 35 percent to 50 percent of time spent on unplanned work.• Some technology deployed.• You have the right vision, but no accountability.• Server-to-admin ratio is way too low.• IT costs too high.• Process subverted by talking to the “right people.”	CLOSED LOOP PROCESS <ul style="list-style-type: none">• 15 percent to 35 percent of time spent on unplanned work.• Some ticketing/work-flow system in place.• Changes documented and approved.• Change success rate is high.• Service levels are pretty good.• Server-to-admin ratio is good, but not best of breed (BoB).• IT costs improving, but still too high.• Security incidents down.	CONTINUOUSLY IMPROVING <ul style="list-style-type: none">• Less than 5 percent of time spent on unplanned work.• Change success rate is very high.• Service levels are world class.• IT operating costs are under control.• Can scale IT capacity rapidly with marginal increases in IT costs.• Change review and learning processes are in place.• Able to increase capacity in a cost effective way.
REACTIVE		USING THE HONOR SYSTEM	CLOSED-LOOP CHANGE MGT	CONTINUOUSLY IMPROVING

Based on the ITPI’s “Visible Ops” framework

GTAG — Three Months Later: Sydney's Story Concludes — 6

When Sydney considers the actions she took based on Jonah's comments and how differently she is managing her organization, she is stunned at the difference in just three months. By focusing on improving how changes are managed, service levels and availability are way up, firefighting is way down, and everyone is feeling more productive because they're spending time on important strategic projects.

The internal auditors are extremely pleased with the progress she's made on her patch management plan. This was unexpected because she now actually patches her systems less often than before the audit! After the audit finding was successfully resolved and validated, Joe, one of the auditors, took her aside and said, "Nice job, Sydney. It looks like you did a complete turnaround in 90 days. That's pretty remarkable. How did you do it?"

Sydney wonders exactly how she did it. She couldn't just say that she did everything that Jonah suggested, because he never really told her what to do. This was immensely frustrating, but it did make her thoroughly revisit her assumptions. After pondering the question awhile, Sydney replies, "I think it happened in three key phases. Do you want me to tell you about it?" Digging out a notebook, Joe smiles excitedly and nods.

Recalling her first meeting with Jonah, Sydney explains, "I came away from that encounter knowing that I had a lot to think about. What was causing the increase in unplanned work? Why were our projects always late and getting later? Was Jonah onto something?"

She asked her staff where they were spending their time. Some parts of her organization were extinguishing fires of the moment and, for whatever reason, could not get on the other side of the proverbial snowball. Many of her impromptu interviews with them were interrupted by a pager beeping, indicating some service outage or interruption, requiring them to cut their conversation short.

She began to wonder what was perpetuating this continued culture of urgency and started following them around to see what they did when they responded to their pagers. For the next two weeks, she spent 50 percent of her time shadowing her managers, trying to form a picture of where they were spending time.

"Closely observing my teams was extremely illuminating. But it was another meeting with Jonah that crystallized my prognosis." Jonah had come back from Europe and told Sydney of the mature and efficient IT processes he had observed in the joint venture partner company his staff was auditing. This European company had some of the best measurement results in the industry, such as low MTTR, high MTBF, change success rates higher than 98 percent, as well as the biggest shocker: high server/system administrator ratios due to performing most of their work in the release management process! He credited part of their success to "managing by fact," a way of operating that enlists the help of everyone in the organization to make their

results visible and thus, difficult to ignore. "When organizations manage by fact," Jonah told her, "nothing is accepted as true without monitoring and measurement."

When she heard about the change success rate measure, Sydney had a light bulb moment. She realized what was creating almost all of the unplanned work: failed changes! Based on what she had observed, she estimated that one of her teams alone was making about 100 changes per week, and for the past week, she could not recall if any of those changes succeeded without causing some rework or unplanned work.

"I think I now better understand the tension when different teams have different definitions of a successful change." She thought about a meeting she'd had with several data center managers at the end of the day when every pager in the room started beeping. One of her managers dryly observed as he headed toward the door, "That must be the developers making their changes before they go home for the day."

She decided to focus on the development team first to find out how many changes they were making, how many of them were failing, and why the changes failed. She asked all of her managers to send a list of the top operational issues that had surfaced in the last quarter and to categorize the root cause as hardware failure, environmental, or change-related. She wanted to find out how the team making those changes decided if they were successful and whether or not they knew that they may have created an urgent firefighting situation for another team.

When she shared an outline of her plan with Jonah, he smiled and said, "Congratulations. You are starting to ask the questions that all high-performing IT organizations have asked!" He asked her what an effective change management process looked like. Sydney was able to identify a few key aspects.

"Great!" Jonah responded. "So what are you going to do to fix your broken processes to achieve your goal?"

Sydney described how her recent efforts allowed her to "stabilize the patient." She reduced or eliminated access to get a grip on the sources of unplanned, error-prone changes. In the prior two weeks, she documented a new change management process, notified all stakeholders, created a change team and change windows to better control what was being done when, and "electrified the fence" to ensure all IT staff felt fully accountable for the "improvements" they have made. Her motto now was "Trust, but verify." People seemed to have gotten the message, and new weekly change management meetings helped her enforce the use of an existing request tracking system and improve internal communications.

Indeed, most of her issues were around failed changes. The new controls were extremely effective. Sydney remembered when she e-mailed her congratulations to the team, announcing that there were no "surprises" in the past five days — a very unusual situation! (When she pulled some

reports to find out when that last occurred, she laughed and decided to keep the results to herself. The last time her service levels were this good was the previous summer when this same team was at an IT offsite, far from their keyboards.)

Sydney now had statistics showing the number of unplanned changes and downtime plus a report with the names of the projects and individuals causing problems since the new process was implemented.

Sydney's staff had identified most causes of downtime and now had a "first response" plan to get equipment up and running in half the time. Her team now needed only 20 percent of the downtime to identify the cause of the outage and spent 80 percent on fixing it. Previously, a great deal of time was spent identifying what was changed, who changed it, and why. Sydney recognized this was inefficient.

"I want to start using change success rate for each business process and IT asset so I can learn from past performance and avoid making historically risky changes." Sydney tells Joe.

Curious about participation of her staff in the new process, Joe asks, "How do you know if everyone is actually following the process?"

Sydney responds by explaining that the IT operations group now publishes a list of authorized changes. Furthermore, she has "electrified the fence" to make sure that the process is followed. She has deployed detective controls to report all production changes, which then must be reconciled with the list of authorized changes. When unauthorized changes are detected, an e-mail is sent to the entire engineering team, telling them that they have four hours for someone to explain why they made a "cowboy change" before we mobilize a security investigation.

Joe asks if everyone develops "rollback" plans before they authorize changes to be made. Sydney confirms this and states that they've seen measurable benefits in defining how to recover from a problem in advance, rather than attempting to do this during the heat of recovery. Joe compliments her, eager to share her successes with several other IT managers, and departs.

Sydney is gratified, but knows she has more to do. She remembers Jonah counseling her: "Now that you've started to control how changes are made in production to reduce the likelihood of unplanned work, you need to inventory all infrastructure assets and identify those that generate the most unplanned work." Just like a wildlife specialist who manages the deer herd, Sydney must "catch and release" or "bag and tag" every asset to figure out what is running, what services depend upon it, who has responsibility for it, and how fragile this artifact is. "Not only does having such an inventory help in problem management, but it aids in developing a repeatable build library for the most critical assets and services, making it much cheaper to fix them."

Sydney agrees that the guidance Jonah provided has helped her understand what Joe is telling her. She looks forward to finalizing her plan of action and discussing it with

Jonah before the next audit committee meeting. "I now see that ineffective change management caused my team to view the process as being bureaucratic, so they ignored it!" Once she was able to show them that 80 percent of their outages were caused by operator and application errors, they began to understand why the department struggled with allocating people to pre-production development projects. Joe thanks Sydney for her time, closes his notebook, and departs.

Sydney is excited about reviewing her plan with the audit committee next week. Based on results of the new change management process during the last 60 days, she estimates redirecting the efforts of two to three people currently handling patch management, plus another person devoted to diagnosing the causes of downtime and steps for remediation.

Sydney believes she can reassign all three staff members to the new customer order Web server project and get it rolled out well before the holidays, instead of the first of the year. "Our marketing people project a 20 percent increase in pre-holiday orders through this process if we are successful. That is good news for the board to hear. And that is just the beginning!" Sydney exclaims to Jonah. "During a recent data center review on noncompliance, your audit team found no discrepancies between our IT configuration standards and our production servers. Not only did my team adopt the new change management process, they installed automated software to prevent and detect variations between standards and current configuration settings — thus significantly improving our information security!"

However, Jonah is not convinced, pointing out that Sydney cannot manage what she does not measure, and that which gets measured gets done. Sydney describes the key measures for her release, controls, resolution, and other processes. She understands that if her staff can't describe their processes and measure against them, they don't know what they're doing.

Jonah looks impressed and says, "Not bad, Sydney. Sounds like a great plan."

For the first time in her conversations with Jonah, Sydney feels as if she's finally passed the test. But she can't resist asking a question that has been on her mind ever since she met Jonah. "By the way, how do you know so much about change management?"

Jonah replies, "As I said before, I'm a business person who just happens to work in internal auditing. At ABC Telecom, I was in IT, responsible for infrastructure and operations. I got that job by demonstrating an ability to install repeatable and verifiable processes, where security, availability, quality, and value were built into the processes and measured in the normal course of business. We couldn't deliver our services and keep our customers without doing this. I took this job to apply the same thought process throughout this company, not just in IT. There is a real need to ensure all of our business processes and supporting systems

GTAG — Three Months Later: Sydney's Story Concludes — 6

contain necessary controls so errors such as vendor overpayments, erroneous financial statements, or late delivery of systems and services do not occur. Where better to do this than in the internal audit department, with the full support of management and the audit committee of the board?"

According to *Enterprise Risk Management – Integrated Framework*, management establishes strategic objectives, selects strategies, and causes aligned objectives to cascade throughout the enterprise. The enterprise risk management framework is geared to achieving an entity's objectives in four categories: strategic, operations, reporting, and compliance. Preventive, detective, and corrective controls should be designed and implemented to help ensure that risk responses are carried out effectively. Auditing can help ensure IT management has an effective process to manage the risks associated with achieving objectives. Examples of the types of change management objectives that IT management needs to define include those for the review and approval of change requests, ensuring changes are made correctly and efficiently, and helping ensure IT can recover quickly when changes fail.

Preventive, detective, and corrective controls should be derived from management's objectives for managing IT changes. IT management should show that the following controls exist and are effective [Tipton 00]:

- Preventive controls.
 - Change authorization.
 - Documentation showing the change management process, including roles and responsibilities of the participants.
 - Documentation showing the authorized owners for all the business processes and supporting IT systems, with assigned levels of authorizations.
 - Separation of roles.
 - Documentation showing clear assignment and separation of roles and responsibilities of the change stakeholders, including change authorization, scheduling, implementation, and review.
 - Clear policies describing the categories and tiers of changes and the levels of formality, approval, and rigor associated with moving changes within each category from the initiation to the implementation stage.
 - Access to make changes in production is strictly limited to those responsible for implementing the changes. All others, such as programmers, do not have such access.
 - Training and awareness programs to promote a culture of change management.
 - Supervision and monitoring.
 - Documentation showing that the change process is being monitored, supervised, and enforced effectively. At any point in time, there should be a published list of authorized changes, as well as a list of unauthorized changes, generated by reconciling actual production changes against the authorized changes.
 - Change management meeting minutes may also show newly authorized and scheduled change

requests. Each change request should have a unique identifier and a responsible individual.

- Detective controls.
 - Supervision and monitoring:
 - Automated methods to detect changes made in production are in place and reviewed independently. These could be audit logs of changes or utilities that scan production infrastructure for changes.
 - Changes to production equipment tracked in work logs, work tickets, and change orders. These should identify the date, time, implementer, and system along with details of the changes made.
 - Changes should be reviewed to ensure there is no variance between the planned change and implemented change. Variances are reported and explained.
 - Acceptance of implemented changes, documenting the correlation between detected changes and implemented changes, indication of successful implementation, acceptance by a change manager, and closure of the change order.
 - Substantive sampling to audit the accuracy of reconciliations between production changes and authorized changes.
 - Sample authorized change requests. Walk through the change management process to ensure that the changes were implemented within the scope of authorized change.
 - Sample detective controls for changes. Ensure that changes can be mapped to authorized work.
- Corrective and recovery controls.
 - Any changes made outside of the change management process are identified. Documentation describes rationale and corrective actions taken.
 - Post-implementation reviews performed of changes made, based on the degree of change, importance of the business activities undergoing change, and significance of the potential risks to the business.
 - When changes fail, problem managers will rule out change first in the repair cycle by accessing authorized and scheduled changes, as well as reviewing production changes on the affected infrastructure.

To be successful, management must be aligned with the concerns of the shareholders, as represented by the board of directors. Enterprise objectives, typically in the form of income/market share targets, business/stock price growth goals, or containment of people and operations costs, must be achieved. Plans to get to the targets must be formulated and rolled out effectively across the entire organization to have a chance for success. The audit committee wants to ensure that management has identified and assessed the risks that could impede achievement of the objectives. Robust processes must be in place to mitigate, manage, accept, or

transfer the risks effectively. Variation from the plan is also a risk that must be managed actively. Internal auditors serve as the eyes and ears of management, seeking out areas in the risk management environment that require strengthening.

For most companies, unavailability of critical services and functions, even for short periods of time, is one of the quickest ways to disrupt progress toward achieving business objectives. Unexpected network downtime can halt the execution of critical business processes such as coordinating materials schedules with suppliers and responding quickly to customer orders. Downtime on critical application, database, or Web servers can be equally destructive. Internal auditors, together with management, want to ensure that these and related risks have been identified and are being measured and managed properly. But how can you manage such risks if you have not identified and analyzed their causes?

Protecting the production environment and supporting the organization as it pursues its business objectives are key responsibilities of the IT department. Internal auditors have the responsibility for ensuring that appropriate risk management processes are in place, including within IT. To this end, the importance of an effective change management process cannot be underestimated, and internal auditors should consider conducting reviews of it on a regular basis.

7.1 Auditing's Role in the Change Management Process

Since internal auditors typically don't have the time to review every facet of the organizations within which they work, they must develop their audit plans based on a risk assessment. To assist in assessing business risk within IT, auditors should gather preliminary information. Here is specifically what auditors should do to determine the relative level of business risk associated with their organization's change management practices and whether to perform a high-level or in-depth review of change management:

1. Understand the basic components of change management. The term *change management*, as used here, does not include the entire systems development lifecycle process, such as application development or configuration management. However, change management must reflect and integrate with the systems development lifecycle process (and companion controls). Understanding the contents of this guide provides you with sufficient background to ask the tough questions of the IT organization to understand the level of improvement that may be needed in its change management process and controls. (Refer to Table 2, page 20, for useful questions to ask.)
2. Use the indicators of effective and ineffective change management processes (refer to Sections 3.2 page 10, and 3.3, page 11) and capability levels provided in this guide (refer to Figure 4, page 23) to assess the relative effectiveness of your organization's change manage-

ment processes. Perform a walk-through of the change management process, and look for the key elements outlined in this guide. Understand how IT management is measuring the process and whether or not the process truly meets the needs of the business.

3. Obtain IT management's scorecard for measuring process results and effectiveness. Determine whether appropriate metrics are being used to monitor the process and drive continuous improvement. (Refer to Table 1, page 16).
4. Determine whether IT management has assigned responsibility for change management to someone other than software developers or others who prepare changes. Has management secured the production environment so that only those responsible for implementing changes can in fact implement changes?
5. Perform a brief review to determine if there are audit trails of changes to the production environment and that the audit trails cannot be manipulated or destroyed.
6. When performing change control audits, look for indicators of effective change management, as illustrated in the sample audit program in Appendix A (page 31). Focus on the risks to the business resulting from the failure to achieve the control objectives, which are based on Control Objectives for Information and Related Technology (COBIT).
7. Assist management in identifying models with which to improve their approach to change management. An example is the *Visible Ops Handbook: Starting ITIL in Four Practical Steps* [ITPI 04], described in Appendix B (page 38). This concise guide is packed with useful information on what a high-performing IT organization looks like and how to improve an underperforming one. It presents the improvement process in four phases:
 - Stabilize the patient.
 - Find fragile artifacts.
 - Create a repeatable build library.
 - Continual improvement.
8. When the organization is considering outsourcing IT functions to a service provider, verify that the organization's expectations are identified clearly in service level agreements (SLAs) and contracts. It is important to ensure that the following issues are taken into consideration regarding the change management process:
 - Who is responsible internally for managing day-to-day changes arising from requests to make changes?
 - How does the organization know when changes are made by the service provider outside of the agreed-upon change management process?
 - What control does the organization have over the service provider to ensure it is not charged for unauthorized or unreasonable changes? How

does the organization know if such changes occur?

- What prevents the provider from approving changes outside of the required change window time periods, with a consequent impact on service (applications not available when needed) and cost (or loss of revenue)?
 - Who is responsible for ensuring that major business changes affecting IT are properly costed, approved, planned, controlled, implemented, and periodically reviewed?
 - Has the provider considered the impacts on infrastructure (system and network) and information security as part of evaluating each change?
 - Has the organization identified who in the organization sits on the provider's change control committees?
 - Who monitors compliance with the SLAs?
 - For systems within the scope of Sarbanes-Oxley Section 404 or other regulations, the SLA also needs to incorporate required practices, validation procedures, timing of the testing required, remediation work, retesting, and other considerations.
9. When discussing and writing audit observations, present the business value of effective change management processes, as well as the risks of ineffective ones. Clearly articulate the operations, financial, and regulatory risks that are not being managed appropriately, and tie the findings to the risk tolerances management has established in support of its business goals and objectives. Avoid focusing on the technology except where certain change management process controls have been automated. Instead, remind management that change management is process-based, with a managerial and human focus, supported with technical and automated controls.

Best in Class Security and Operations Round Table Report, Julia Allen, Kevin Behr, Gene Kim, et al, (CMU/SEI-2004-SR-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, March 2004. Available from the authors, by request.

Capability Maturity Model® Integration (CMMI®). Carnegie Mellon University, Software Engineering Institute. Available at <http://www.sei.cmu.edu/cmmi/cmmi.html>. Chrissis, Mary Beth, et al. *CMMI®: Guidelines for Process Integration and Product Improvement*. Addison Wesley, 2003. Specifically refer to the configuration management process area.

COBIT [Control Objectives for Information and related Technology] 3rd Edition Executive Summary, Framework, Control Objectives, Audit Guidelines, and Management Guidelines, July 2000. Available at <http://www.itgi.org> and <http://www.isaca.org>. Specifically refer to AI-6: Acquisition and Implementation: Manage changes, and DS-9: Delivery and Support: Manage the configurations.

Information Technology Infrastructure Library (ITIL)® 11. Office of Government Commerce. Refer to <http://www.ogc.gov.uk/index.asp?id=2261> and <http://www.itsmf.com>. Specifically refer to the volume *Best Practice for Service Support*, Chapter 8, Change Management (2000).

ISO/IEC 17799 Information Technology Code of Practices for Information Security Management, First Edition. ISO/IEC 17799:2000(E). December 2001. Specifically refer to Sections 8.1.2 Operational change control, 10.5.1 Change control procedures, 10.5.2 Technical review of operating system changes, and 10.5.3 Restrictions on changes to software packages.

Microsoft Service Management Functions Operations Guide: Change Management. Microsoft Corp., 2004. Available at <http://www.microsoft.com/technet/itsolutions/techguide/msm/smf/smfchgmg.mspx>.

Systems Assurance and Control (SAC). The Institute of Internal Auditors Research Foundation, August 2003. Information and table of contents available at <http://www.theiia.org/esac/index.cfm>.

Visible Ops Handbook: Starting ITIL in Four Practical Steps. Kevin Behr, Gene Kim, George Spafford. IT Process Institute, 2004. Information is available at <http://www.itpi.org/visibleops>.

¹¹ ITIL is a registered trademark of the Office of Government Commerce (OGC).

Process, Purpose, and Risks

IT change management is a process to manage changes to production hardware, network devices, operating systems, and application software. An organization's management uses the IT change management process to:

- Ensure IT changes meet the organization's needs and create business value.
- Anticipate and manage problems that may be introduced in the production environment as a result of changes.
- Promote the effectiveness and efficiency of IT change management efforts.

Achievement of these high-level strategic and operational objectives is not automatically assured. Events, key risks, and other circumstances could prevent management from achieving desired business benefits. Such events include:

- Changes disrupt operations or create other problems.
- Changes cause disruptions or other problems are not detected or traced to their source for timely identification of causes and restoration of affected services.
- Changes are not performed in a timely or complete manner.
- Changes are not made in the most efficient manner, resulting in excessive costs.
- Changes, although properly implemented, fail to meet business requirements and thus do not create the desired business value.

Below is a sample audit program that may be useful to IT management and internal auditors to assess the controls that should mitigate the risk inherent in these events.

9.1 Change Management Definitions¹²:

- Change request: The proposed procedure for an addition, modification, or removal of approved, supported, or baselined hardware, network, software, application, environment, system, desktop build, or associated documentation. [ITIL 00]
- Authorized change: A change request for a change procedure that has been approved by the change advisory board (CAB).
- Unauthorized change: A detected change from the production detective controls that cannot be mapped to an authorized change. Examples of variance that would result in an unauthorized change include:
 - Who: the change was implemented by an unauthorized individual.
 - What: the change exceeds the scope of authorized change or incompletely implemented the intended change.

- Where: the change was made to an inappropriate asset.
- When: the change was made outside the scheduled change window or maintenance window.
- Planned work: Any worker activity that can be mapped to an authorized project or procedure.
- Unplanned work: Any worker activity that cannot be mapped to an authorized project or procedure.¹³
- Service-affecting incident: Any event that is not part of the standard operation of a service and that causes, or may cause, an interruption to, or a reduction in, the quality of that service. Examples include application or service not available, hardware or system down, service impairment, etc. [ITIL 00]

¹² If management does not have their own definitions, the auditor and auditee should agree on what the definitions are for the purpose of the audit.

¹³ Ideally, planned and unplanned work is measured, not calculated. However, even using the most informal definitions, the amount of planned and unplanned work can serve as excellent indicators of the effectiveness of the IT organization. Any service interruption represents unplanned work, as would the work resulting from a failed change, emergency change, patch or security incident. Unplanned work is what causes IT managers to rearrange their schedule and prevents system administrators from being able to do daily plans.

GTAG — Appendix A — IT Change Management Audit Program — 9

Table 3: IT Change Management Audit Program

Risk	Control Objective	Test	COBIT Reference
		<p>Obtain:</p> <ul style="list-style-type: none"> • IT change management policies, standards, and procedures. • Listing of personnel and departmental organization chart(s) showing participants in change management, especially those responsible for developing and implementing changes. • Information regarding third-party service providers involved in the process, including relevant SLAs and contracts. • Workflow diagrams depicting the IT change management process. • Inventory and descriptions of production environment elements in scope (for example, network devices, servers, libraries, databases). • IT operations metrics, standards, and service level commitments, especially those directly relating to change and problem management. • Sample reports showing how metrics, standards, and service level commitments are reported to management. • Service desk problem reports and analyses. • List of authorized changes. • Change control logs. 	
<p>The IT change management process may not adequately serve business goals.</p>	<p>IT management ensures that all requests for changes, system maintenance, and supplier maintenance are standardized and are subject to formal change management procedures. Management has adequate visibility of, and exercises adequate control over, changes to the production IT environment.</p>	<p>Determine that IT change management policies, standards, and procedures apply broadly enough to ensure management control of the production environment. Ensure they provide for:</p> <ul style="list-style-type: none"> • Differing paths depending on costs and risks of change. • Business case information to guide prioritization of change efforts. • Structured risk and impact assessment considering all possible impacts on the operational system and its functionality. • Categorization and prioritization of changes. • Specific handling of emergency changes. • Communication to change requesters regarding the status of their request. • Requirements definition. • Testing (including unit, regression, system, integration, capacity/performance, and user acceptance testing as appropriate). 	<p>AI6. Manage Changes</p>

GTAG — Appendix A — IT Change Management Audit Program — 9

Table 3: IT Change Management Audit Program (cont'd)

		<ul style="list-style-type: none"> • Appropriate generation and/or modification of related documentation. • Adequate communication of pending changes to affected parties, including management, users, developers, security administrators, IT operations, and help desk staff. • Appropriate segregation of development, test, and production environments. • Adequate consideration of controls implications (for example, including information security management early on). • Adequate consideration of business continuity effects. • Responsibilities for investigating failures, together with the incident resolution process. • Controls defined throughout the process of change. 	
		<p>Review IT operations metrics, standards, service level commitments, and related reports. Ensure that these provide management with independent, timely, accurate, complete, concise, and relevant information to determine the effects of changes and problems on IT operations and ultimately on business goals. Measures should include:</p> <ul style="list-style-type: none"> • Number of changes authorized per week – How many changes, as measured by the change management process? (In general, higher is better, as long as the change success rate remains high as well.) • Number of actual changes made per week – How many changes, as measured by detective controls? (In general, higher is better, but, this should not be higher than the changes authorized by the change advisory board!) • Number of unauthorized changes – How many changes circumvented the change process? This is typically measured by using the detective controls, or worse, through unplanned outages. (Lower is better.) • Change success rate – How many changes are successfully implemented without causing an outage or episode of unplanned work? (Higher is better: Best in class does better than 99 percent.) • Number of service-affecting outages – How many changes result in service impairment or an outage? (Lower is better.) • Number of emergency changes – How many changes required using the emergency change process? (Lower is typically better, because it indicates a higher percentage of planned work.) 	

GTAG — Appendix A — IT Change Management Audit Program — 9

Table 3: IT Change Management Audit Program (cont'd)

		Through interviews, observation, or review of meeting records, verify that there is a management group such as a change advisory board that meets regularly, reviews IT change requests, and approves or disapproves them as appropriate. Determine that the membership provides management with adequate understanding of, and control over, changes. Ensure that users are included where appropriate.	AI6.2 Impact Assessment
		Obtain listings of personnel and copies of organization charts showing the group responsible for managing and implementing IT changes. Ensure the group is independent of those responsible for requesting and developing/ preparing changes.	AI6.6 Authorized Maintenance
		Select a sample of changes made to production elements in scope during the audit period. Determine that there is clear documentation indicating that all applicable policies, standards, and procedures were followed in implementing the changes.	AI6.1 Change Request Initiation and Control
IT changes that do not meet management's business needs may be implemented.	Only appropriate changes are approved.	Review policies, standards, and procedures to determine that changes require management approval, including management approval of business users and IT operations. Approval should be required at appropriate points in the change process. For example, approval may be required by appropriate management at the end of business case preparation, initial requirements definition, and/or certain testing phases.	AI6.2 Impact Assessment
		Review IT change management standards, procedures, practices, and technologies to ensure that before final approval, requirements: <ul style="list-style-type: none"> • Are verified as meeting the business case for the change. • Have been met as evidenced by the testing. 	
		Review IT change management standards, procedures, practices, and technologies to ensure that before final approval, testing has adequately demonstrated the change will not harm the production environment.	AI6.7 Software Release Policy
	Only approved changes are implemented.	Obtain access control information for (a sample of) production source and executables. Ensure that only those responsible for implementing changes can modify, append, or delete these.	AI6.6 Authorized Maintenance
		Review policies and standards to determine that they require reliable, easily-reviewed audit trails of changes to production elements.	
		Review audit trail technology and related processes. No individual should have ongoing access rights to delete or modify the audit trails. The audit trails should be managed so as to keep them available for convenient review in the short term and for investigation in the long term.	
		Review procedures for reviewing audit trails of changes to production elements in scope. Ensure they require timely, independent review, follow-up of exceptions, and evidence of review.	

GTAG — Appendix A — Change Management Audit Program — 9

Table 3: IT Change Management Audit Program (cont'd)

		Review change management standards, procedures, practices, and technology to determine that controls ensure that the components implemented into production are the same as the components developed, tested, and approved.	AI6.3 Control of Changes
		Review change management standards, procedures, practices, and technology to determine that controls ensure that source and executables implemented into production match one another.	AI6.3 Control of Changes
	Implemented changes meet business requirements.	Review IT change management policies, standards, and procedures to determine whether changes of significant cost or risk require approval by business users at appropriate points.	AI6.1 Change Request Initiation and Control
		Through interviews and reviews of documentation, determine that for each significant change, a post-implementation review assesses its effectiveness and measures it against the business case applied in initiating the change.	
IT changes may cause production problems.	IT changes are implemented in appropriate sequence without interfering with other changes.	<p>Review change management standards, procedures, practices, and technology to determine that controls ensure:</p> <ul style="list-style-type: none"> • Changes are implemented periodically as releases rather than as isolated modifications to the production environment. • Changes that may affect one another are synchronized appropriately (for example, only one programmer at a time is modifying a given module). 	AI6.7 Software Release Policy
	Changes are implemented accurately and as intended.	Ensure that change management and software control and distribution are integrated properly with a comprehensive configuration management system.	AI6.3 Control of Changes
		Review IT change management policies, standards, and procedures to ensure that changes adequately document the steps needed to implement the change.	
		Ensure that the system used to monitor changes to application systems is automated to support the recording and tracking of changes made to large, complex information systems.	AI6.3 Control of Changes
	IT operations can recover efficiently and effectively from change-related problems.	Review IT change management policies, standards, and procedures to ensure that changes must have adequate backout documentation before being staged to production.	
		Review IT change management policies, standards, and procedures to ensure that changes must thoroughly document what was changed, when and by whom. Each change must carry an accurate disposition at all times (for example, in development, implemented, backed out, canceled, etc.) This documentation must be reliably accurate and easily accessible.	AI6.3 Control of Changes

GTAG — Appendix A — IT Change Management Audit Program — 9

Table 3: IT Change Management Audit Program (cont'd)

Production operations may not recover efficiently from problems caused by changes.	Change and problem management processes are integrated.	Review change management standards and procedures to make sure each change explicitly records any problem(s) it is designed to address.	
		Review problem management standards and procedures to make sure each problem record explicitly records any change found to have caused or contributed to the problem.	
Changes that must be implemented faster than the normal change cycle allows may bypass and/or compromise change controls.	Emergency changes are implemented in a way that preserves change controls.	Determine that IT change management policies, standards, and procedures establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational and management assessment prior to implementation.	AI6.4 Emergency Changes
		Review emergency change procedures to make sure emergency changes can be implemented quickly, effectively, and in a way that preserves accountability, traceability, and independent review.	
		<p>Select a sample of emergency changes during the audit period and ensure that:</p> <ul style="list-style-type: none"> • The change was needed for a true emergency. • Emergency procedures were followed. • They were recorded and authorized by IT management prior to implementation. • Appropriate management of affected areas was notified promptly. • Unapproved changes were detected, and exceptions were raised and resolved promptly. • Any necessary cleanup was completed promptly • User manuals were updated with changes affecting the user interface, the program functioning, security, and other changes. 	AI6.4 Emergency Changes

GTAG — Appendix A — IT Change Management Audit Program — 9

Tables 4 and 5 show typical roles and the titles associated with them, as well as duties that should not be combined. Auditors will quickly recognize the parallels of these guidelines and typical transaction processing guidelines. For instance, those who manage the infrastructure should not audit it. Those who implement change should not approve change. Those who write the application should not test it, run it, or operate it.

As noted in Section 4.5 “Integrating Patch Management Into Change Management,” (page 18) the more complex and dynamic the IT production environment, the greater the need for effective controls. As the number of change implementers and rates of change increase, so does the need for automated and independent monitoring and oversight.

Table 4: Typical Roles

Roles in the Change Lifecycle	Typical Titles and Roles
Change requester	Business unit, IT operations, security, service manager.
Change preparer	R&D, database administrator, application development team, application programmer. Quality assurance, build and staging team, pre-production team, platform team.
Change approver	Change manager, change advisory board, change control committee, change management board.
Change implementer	IT operations, network operations, network engineering, systems administrators, security.
Change reviewer	IT operations management, change advisory board, security, auditing.
Change audit	IT operations management, change advisory board, security, auditing.

Table 5: Segregation of Duties

For each change...	Should be independent of...
Implementers	Requesters
Operators of the production environment	Preparers
Tester	Preparers
Implementers	Preparers
At least one approver	Preparers
At least one approver	Requesters
At least one approver	Implementers
Reviewers	Implementers
Audit	All of the above

Sources: COBIT Control Objectives, 3rd Edition, July 2000: Planning & Organization 4 (P04), page 42, ISO/IEC 17799:2001, Auditors Guide, Section 8.1.4. Segregation of Duties

The Visible Ops methodology, published by the ITPI, provides guidance for IT managers on how to build auditable and catalytic processes in four phases. The first phase builds a sustaining change management process by attacking the highest contributor to unplanned work (i.e., self-inflicted outages, long repair times due to absence of change information). To “stabilize the patient,” we do the following:

1. Reduce or Eliminate Access: Clear everyone away from the asset unless they are formally authorized to make changes. Because these assets have low change success rates, we must reduce the number of times the dice are rolled.
 - a. Document the New Change Policy: Our recommended change policy is very simple: “Absolutely no changes to this asset unless authorized by me.” This policy is our preventive control and creates an expectation of behavior.
 - b. Notify Stakeholders: After the initial change policy is established, notify all the stakeholders about the new process. Make sure the entire staff sees it. E-mail it to the team. Print it out. Add it to login banners. Post it on the Web site or intranet portal home page.
2. Electrify the Fence: To enforce the new change management process, we must electrify the fence to ensure that all production changes are detected and correlated against authorized changes. When unauthorized changes are detected, use them to reinforce the change process, and reinforce it constantly. For example, “Team, let me be clear on this: These processes are here to enable the success of the entire team, not just individuals. So, anyone making a change without getting authorization undermines the success of the team, and we’ll have to deal with that. At a minimum, you’ll have to explain why you made your cowboy change to the entire team. If it keeps happening, you may get the day off, and eventually, it may prevent you from being a part of this team.”
3. Modify First Response: The Catalytic Key: To ensure that the change management process returns value back to the organization, integrate the change management process into the problem management function. Ensure that problem managers have all change-related information when they are working problems. Because 80 percent of outages are due to change and 80 percent of MTTR is spent trying to discover what changed, having this information at hand ensures all relevant and causal evidence is already available. Typically, when equipped in this way, problem managers can diagnose issues successfully without logging into any infrastructure more than 50 percent of the time.
4. Create the Change Team: In the previous steps, we have started to specify the correct path for change and

built the mechanisms to ensure that the process is being followed. In this step, we create the correct path to go from desired change to authorized change. We create a change advisory board (CAB), comprised of the relevant stakeholders of each critical IT service. These stakeholders are the people who can best make decisions about changes because of their understanding of the business goals, as well as technical and operational risks.

5. Create a Change Request Tracking System: A prerequisite for any effective change management process is the ability to track requests for changes (RFCs) through the authorization, implementation, and verification processes. Paper-based manual systems quickly become impractical when the organization is large or complex, or when the number of changes is high. Because of this, most groups use some computerized means to track RFCs and assign work order numbers. Some refer to these applications as “ticketing systems” or “change workflow systems.” However you track the changes, don’t let the use of technology supplant the need for a strong process.
6. Start Weekly Change Management Meetings (To Authorize Change) and Daily Change Briefings (To Announce Changes): Now that we have identified the change stakeholders by creating the CAB, the next step is to create a forum for them to make decisions on requested changes. The CAB will authorize, deny, or negotiate a change with the requester. Authorized changes will be scheduled, implemented, and finally verified. The goal is to create a process that enables the highest successful change throughput for the organization with the least amount of bureaucracy possible. Although they may seem unnatural at first, with practice, weekly 15 minute change management meetings are possible. Take special care to avoid an attitude of “just get it done,” which allows people to make changes that circumvent the change approval process. If we make it easy for all changes to flow through our process, it will soon be easier to use the process than to circumvent it, even during emergencies.

Following the Visible Ops methodology will help you build a sustainable change management process that quickly identifies and corrects the causes of poor change success rates.

GTAG — Appendix C — Example Business Case for Change Management — 11

High-performing organizations use their IT change management processes to reduce risk, increase operational effectiveness, and increase operational efficiency. Thus, the benefits of effective change controls are significant and measurable. Being able to demonstrate this eases the task of building a business case for improving change controls, as opposed to

doing it “just to make auditing happy.” As described in previous sections, the key operational metrics are change failure rate, recovery time in the case of failed changes, and the resulting unplanned work. Table 6 summarizes indicators of ineffective change management. Table 7 describes ways in which to address these based on actual field experience.

Table 6: Issues and Indicators of Ineffective Change Management

Our Symptoms	Underlying Causes
“Like many large IT organizations, we were experiencing the effects of undocumented changes. We knew they were occurring, but they were difficult to track down, and in today’s security-conscious atmosphere, this was not acceptable.”	<p>Poor service levels and availability.</p> <p>Unknown number of operational changes.</p> <p>Uncontrolled rate of change.</p> <p>Low changes success rates (less than 70 percent).</p> <p>High amounts of unplanned work (less than 40 percent).</p>
“In outage scenarios for the fixed incoming trading systems, the help desk was the first to know. These would get escalated to the IT management group, who would form a response team and do the archaeology to find out what happened.”	<p>When changes fail, investigating causes and problem management consumed over 25 percent of the workload.</p> <p>Inaccurate diagnosis leads to poor first fix rate (FFR less than 50 percent).</p>
“It was like the Wild West. People were not documenting their changes, let alone getting approval. You could tell from our availability statistics!”	<p>Absence of detective controls around change management processes leads to poor performance.</p> <p>Absence of change controls prevents proof of preventive and detective controls for auditors to attest that controls are effective.</p>

Table 7: Benefits From Effective Transformation (based on actual reported results)

Our Remedy	Benefits
“We realized that unexpected consequences of changes were the highest contributor to unplanned work. We formalized the approval required to make production changes and to put teeth in the process. We also ‘electrified the fence’ to ensure that the change management process is being followed.”	<p>Increased management visibility of proposed changes.</p> <p>Operational changes are only those authorized by the change management process.</p> <p>Increased control of change rate can lead to change success rate increases to > 95 percent, due to visibility and testing.</p>
“We started to create real accountability for everyone to follow the change management process. We chose our daily availability management meetings (“the DAMM meetings”), chaired by Kenny, our vice president of operations. Kenny reviews all failed changes with the change implementers and has a special session for anyone who went around the change management process. Let’s just say that unauthorized changes and cowboy changes happen much less often!”	<p>(This particular business calculates downtime cost at \$7,000 per minute.)</p> <p>Number of unauthorized changes declined from “several per day” to “several per year.” Because each outage required two work hours to restore service (a conservative estimate), on an annualized basis, 5,000 work hours was averted.</p> <p>All changes are fully documented, allowing changes to be ruled out first in the problem repair cycle, allowing restoration time to go from “hours” to “minutes.” For the 11 outages in Q3, this saved about 13 hours of system downtime.</p>

GTAG — Appendix C — Example Business Case for Change Management — 11

Table 7: Benefits From Effective Transformation (based on actual reported results) (cont'd)

Our Remedy	Benefits
<p>"We realized that unexpected consequences of changes were the highest contributor to unplanned work. We wanted to better enforce our standards and be able to eliminate the time spent on detective work.</p> <p>"Furthermore, preparing for audits went from four work weeks each year per project to being ready for each audit in less than half a day!</p> <p>"Lastly, we used to have three different compliance teams: one for Sarbanes-Oxley Section 404, Gramm-Leach Bliley Act, and Health Insurance Portability and Accountability Act. When we realized that all of them required effective reporting on change controls, we replaced all those teams into one chartered with compliance for all three."</p>	<p>Regulatory compliance is now handled as a day-to-day matter, instead of last-minute crash preparation.</p> <p>Because proof of effective change controls is being generated regularly, no management comment letters were generated by the external auditors (compared to last year, they averted the 130 work hours of unplanned work and audit fees).</p> <p>Mapping change controls to common regulatory requirements reduces the amount of duplicate work done by separate teams. Twelve IT staff members have been re-assigned to the IT operations team.</p>
<p>"In addition to all of us not having to wear pagers home, we're finding that we have much more time to work on planned projects, as opposed to firefighting all the time."</p>	<p>Unplanned work reduced from more than 40 percent to 15 percent.</p> <p>On-time project deliveries went from zero to 60 percent.</p> <p>The CIO has tasked the IT management group with the key strategic projects for the following year.</p>

Here are some widely-used tools to automate the processes described in this guide:

- *Visible Ops Handbook: Starting ITIL in Four Practical Steps.*
- Change management workflow (preventive control).
 - BMC/Remedy Action Request System.
(<http://www.remedy.com/solutions/coretech/index.html>)
 - HP Service Desk.
(<http://managementsoftware.hp.com/products/sdesk/index.html>).
- Change auditing and monitoring (detective control).
 - Tripwire for Servers and Networking Devices
(<http://www.tripwire.com>)

Materials for the sample audit guide presented in Appendix A were, in part, taken from <http://auditnet.org/asapind.htm>.

[Allen 04] Allen, Julia; Behr, Kevin; Kim, Gene et al. *Best in Class Security and Operations Round Table Report* (CMU/SEI-2004-SR-002). Pittsburgh, PA: Software Engineering Institute, Carnegie Mellon University, March 2004. Available upon request.

[BDO 04] BDO Seidman LLP, et al. *A Framework for Evaluating Control Exceptions and Deficiencies*. BDO Seidman LLP, Crowe Chizek and Co. LLC, Deloitte & Touche LLP, Ernst & Young LLP, Grant Thornton LLP, Harbinger PLC, KPMG LLP, McGladrey & Pullen LLP, PricewaterhouseCoopers LLP, Dec. 20, 2004. Available at various sites including http://www.kpmg.com/Rut2000_prod/Documents/9/US_DPP_ICOFR_04_024_A01.pdf.

[BITS 04] BITS Financial Services Roundtable. *Patch Management Best Practices for IT Service Providers*. BITS, July 2004. Available at <http://www.bitsinfo.org/bitspatch-mgmt2004.pdf>.

[Chambers 03] Chambers, Andrew. Tolley's *Corporate Governance Handbook: 2nd Edition*, Appendix B: Fraud. Lexis Nexis, 2003.

[CISWG 04] Corporate Information Security Working Group. Subcommittee on Technology, Information Policy, Intergovernmental Relations & the Census Government Reform Committee, U.S. House of Representatives. *Report of the Best Practices and Metrics Teams*. Nov. 17, 2004. Available upon request.

[COSO 04] The Committee of Sponsoring Organizations of the Treadway Commission. *Enterprise Risk Management – Integrated Framework*. September 2004. The executive summary and ordering information is available at <http://www.coso.org>.

[Gartner 03] Series on Change Management:

- Brittain, Kris. *Change Management Makes an Impact on IT Service Quality*. Note AV-19-3311, Gartner, March 13, 2003.
- Scott, Donna; Brittain, Kris. *Defining IT Change Management*. Research Note COM-19-1428, Gartner, March 6, 2003.
- Brittain, Kris; Scott, Donna. *Critical Factors Powering Operational Change Management*. Research Note DF-18-4179, Gartner, March 4, 2003.
- Scott, Donna; Brittain, Kris. *Best Practices for Operational Change Management*. Commentary COM-19-1253, Gartner, March 6, 2003.
- Brittain, Kris; Scott, Donna. *Governance/Policy Back Operational Change Management*. Commentary COM-18-4180, Gartner, March 6, 2003.

[Gall 86] Gall, John. *Systemantics: The Underground Text of Systems Lore*, General Systemantics Press, 1986.

[Goldratt 92] Goldratt, Eliyahu; Cox, Jeff. *The Goal: A Process of Ongoing Improvement*, 2nd Rev edition, North River Press, May 1992.

[Hulme 04] Hulme, George. "Federal CISOs Rank Patch Management As Biggest Obstacle." *InformationWeek*, Nov. 22, 2004. Available at <http://informationweek.com/story/showArticle.jhtml?articleID=53701321>.

[ITIL 00] Information Technology Infrastructure Library (ITIL)[®]14. Office of Government Commerce. Refer to <http://www.ogc.gov.uk/index.asp?id=2261> and <http://www.itsmf.com>. Specifically refer to *Best Practice for Service Support*, Chapter 8 Change Management (2000).

[ITPI 04] Behr, Kevin; Kim, Gene; Spafford, George. *Visible Ops Handbook: Starting ITIL in Four Practical Steps*. IT Process Institute, 2004. Introductory and ordering information is available at <http://www.itpi.org>.

[Kim 03] Kim, Gene. "High-Performing IT Operations and Security Workshop Findings: Part 1." *ComputerWorld*, December 2003. Available at <http://www.computerworld.com/securitytopics/security/story/0,10801,91205,00.html?nas=SEC2-91205>.

[Mair 73] Mair, William; Wood, Donald; Davis, Keagle. *Computer Control and Audit*. Touche Ross & Co., 1972, 1973, 1976, and 1978. Formerly distributed by The Institute of Internal Auditors, Inc. No longer in print.

[O'Reilly 98] O'Reilly, Vincent; McDonnell, Patrick; Winograd, Barry; Gerson, James; Jaenicke, Henry. *Montgomery's Auditing, 12th Edition*. Wiley, 1998.

[PWC 04] PriceWaterhouseCoopers. *The Discipline of Enterprise Patch Management: A Critical Component of a Broader Approach to Protection*, 2004. Available at <http://www.pwcglobal.com/extweb/manissue.nsf/DocID/5BF8D134DFEE39A385256E5F006A0F89>.

[Salamasick 03] Salamasick, Mark. *PC Management Best Practices – A Study of the Total Cost of Ownership, Risk, Security, and Audit*. The Institute of Internal Auditors Research Foundation, November 2003. Ordering information available at http://www.theiia.org/iiabookstore.cfm?fuseaction=product_detail&order_num=482.

[Tipton 00] Tipton, Hal, Miki Kraus. *Handbook Information Security Management*. Auerbach Publications, 2000.

Julia H. Allen is a senior member of the technical staff within the Networked Systems Survivability Program at the Software Engineering Institute (SEI), a unit of Carnegie Mellon University in Pittsburgh, PA. The CERT® Coordination Center is also a part of this program.

Allen is engaged in developing and transitioning enterprise security frameworks and executive outreach programs in enterprise security and governance. Prior to this technical assignment, Allen served as acting director of the SEI for an interim period of six months as well as deputy director/chief operating officer for three years. Her degrees include a B. Sci. in Computer Science (University of Michigan) and an MS in Electrical Engineering (University of Southern California). She is the author of *The CERT Guide to System and Network Security Practices* (Addison-Wesley, June 2001).

Contact Information:

Carnegie Mellon University
Software Engineering Institute
4500 Fifth Ave.
Pittsburgh, PA 15213 USA
jha@sei.cmu.edu, jha@cert.org

Glenn L. Hyatt, CIA, CISA, CISSP is data security manager for General Motors Acceptance Corp. (GMAC) Mortgage, where he manages information security operations and investigations. Hyatt has served for more than 20 years in IT-related positions, starting as a programmer, then moving into information security management, IT consulting, and IT audit management. He previously held positions at the Federal Reserve Bank of Philadelphia, Citibank, and Ernst & Young and holds a Master of Science degree in Computer and Information Sciences from the University of Delaware.

Contact Information:

GMAC Mortgage
4 Walnut Grove Dr., 190-400-215
Horsham, PA 19044 USA
+1-215-682-3424
Glenn.Hyatt@gmam.com

Gene H. Kim, CISA, is the chief technology officer (CTO) and founder of Tripwire Inc. In 1992, he co-authored Tripwire while at Purdue University with Dr. Gene Spafford. In 2004, he wrote *The Visible Ops Handbook* and co-founded the IT Process Institute, dedicated to research, benchmarking, and developing prescriptive guidance for IT operations and security management and auditors. He is currently actively working with the Software Engineering Institute and The Institute of Internal Auditors to capture how “best in class” organizations have IT operations, security, management, governance, and auditing working together to solve common business objectives. Gene is currently serving on The IIA’s Advanced Technology Committee.

Gene holds an M.S. in computer science from University of Arizona and a B.S. in computer sciences from Purdue University. Most recently, Gene was named one of the “Top 4 CTOs to Watch” by *InfoWorld* magazine due to his “forward-thinking and leading-edge activities.” He also served as co-chair of the April 2003 SANS technical workshop called Auditable Security Controls That Work, hailed by SANS as one of their top five gifts back to the community and one of their top initiatives for 2003. Gene co-chaired the Best in Class Security and Operations Roundtable (BIC-SORT) with the Software Engineering Institute in October 2003. Gene is certified on both IT management and audit processes, possessing both ITIL Foundations and CISA certifications.

Contact Information:

Gene Kim
Tripwire Inc.
326 SW Broadway Ave., 3rd Floor
Portland, OR 97205 USA
+1-503-276-7676
genek@tripwire.com

Jay R. Taylor, CIA, CFE, CISA, is general director of Information Technology Audit for General Motors Corp., and is responsible for assessing risks and providing global internal audit and consulting services regarding General Motors and General Motors Acceptance Corp. business units and joint ventures worldwide. GM operates in a highly leveraged environment using numerous third-party IT providers around the world. Taylor earned his MBA from the University of Michigan and is active in The Institute of Internal Auditors, currently serving on the International Advanced Technology Committee. He previously served on the International Educational Products Committee of The IIA, and is past president of The IIA’s Mid-Michigan Chapter and a former member of the Detroit Chapter Board of Governors. Recent professional contributions include presentations made to the 2004 IIA Enterprise Risk Management Conference and the 2004 IIA Emerging Trends and Leading Practices Conference.

Contact Information:

General Motors Corp.
300 Renaissance Center
Mail Code 482-C18-B76
Detroit, MI 48265-3000 USA
+1-313-665-3700
jay.r.taylor@gm.com

BMC Software

Although Sarbanes-Oxley Section 404 does not mandate systems-based controls to meet general IT control objectives, in some cases, using software-based solutions is the best way to implement consistent and cost-effective controls.

BMC Software, a leading provider of IT systems and service management solutions, offers systems-based controls that address some of the most challenging controls objectives.

Identity and Access Management Controls – enable centralized and delegated management of identities and access privileges, single sign-on for Web and non-Web environments, self-service password management, auditing and reporting capabilities, and automatic notification and corrective actions in response to access policy violations.

Data Management and Recovery Controls – support both mainframe and distributed environments. They include monitoring and performance tuning, data change management, database security management, backup and recovery, and database archiving.

Change and Configuration Controls – provide a comprehensive and flexible solution for controlling both infrastructure and application change process from request and planning through implementation and verification.

BMC Software Inc. [NYSE:BMC], is a leading provider of enterprise management solutions that empower companies to manage their IT infrastructure from a business perspective. Delivering Business Service Management, BMC Software solutions span enterprise systems, applications, databases, and service management. Founded in 1980, BMC Software has offices worldwide and fiscal 2004 revenues of more than \$1.4 billion.

For more information about BMC Software, visit www.bmc.com/compliance.

Tripwire Inc.

Tripwire is the first company to recognize the importance of securing the integrity of the network and pioneered change monitoring as a foundational IT control. Our goal is to help organizations audit change to prove control of their IT infrastructure.

Every IT organization is challenged to help its company maintain compliance with regulatory requirements while assuring security and availability. IT risk increasingly is impacting the overall business risk of an organization. The single greatest contributor to IT risk is change — unknown and uncontrolled change. As part of a comprehensive change management system that includes IT process controls — preventative, detective, and corrective — detective control is the most critical. The ability to detect change enables the IT team to monitor and enforce processes, while overall improving security.

In today's IT audit and compliance-driven environment, responsibility for correcting deficiencies in internal process controls rests squarely on the shoulders of IT, making change auditing capabilities a major and immediate requirement. Tripwire's automated detection, reconciliation, and reporting capabilities allow IT organizations to segregate people and processes that initiate change from those that monitor and report on change. This control of independence is an important element of most compliance requirements, and it is a key reason why more than 4,500 customers worldwide look to Tripwire to manage their change auditing needs.

Tripwire Inc is a proud sponsor of the GTAG series.

Project Review Team

Jennifer Bayuk, Bear Stearns

Rod Brennan, Siemens

Larry Brown, Options Clearing Corporation

Claude Cargou, AXA

Angelina Chin, General Motors Corporation

James Christiansen, Experian

Ed Hill, Protiviti

Clint Kreitner, Center for Internet Security

Charlie LeGrand, CHL Associates

Sydney Leo, KPMG

Warren Malmquist, Coors

Norman Marks, Maxtor

Stuart M. McCubbrey, General Motors Corporation

Heriot Prentice, The Institute of Internal Auditors

Michael Prospect, SIAC

Mark Salamasick, Univ of Texas

Bill Shinn, Washington Mutual

Matt Snyder, General Motors Corporation

Jon Stanley, General Motors Corporation

Carol Woody, Carnegie Mellon University, Software Engineering Institute



Information Technology Controls

This guide focuses on how IT roles and responsibilities are dispersed throughout the organization, how accurate assessment of IT controls is achieved, and how an organization can promote IT reliability and efficiency.

What is GTAG?

Prepared by The Institute of Internal Auditors, each Global Technology Audit Guide (GTAG) is written in straightforward business language to address a timely issue related to information technology management, control, or security. GTAG is a ready resource series for chief audit executives to use in the education of members of the board and audit committee, management, process owners, and others regarding technology-associated risks and recommended practices.



**The Institute of
Internal Auditors**

Order Number: 1009
IIA Member US \$25
Nonmember US \$30
IIA Event US \$22.50

ISBN 0-89413-574-0

