GTAG®

GLOBAL TECHNOLOGY AUDIT GUIDE

IPPF – Practice Guide

Change and Patch Management Controls: Critical for Organizational Success

2nd Edition

The Institute of Internal Auditors

Global Technology Audit Guide (GTAG®) 2
Change and Patch Management Controls: Critical for Organizational Success

2nd Edition

March 2012

GTAG — Table of Contents

Executive Summary

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

IT change and patch management can be defined 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 (e.g., applications, operating systems, and databases).
- Infrastructure changes (e.g., servers, cabling, routers, and firewalls).

Stable and managed IT production environments require that implementation of changes be predictable and repeatable, as well as follow a controlled process that is defined, monitored, and enforced. Segregation of duties (e.g., separation of preparer, tester, implementer, and approver roles) and monitoring controls will reduce the risk of fraud and errors in the process.

Internal auditors should be familiar with key controls in the IT change management process, including:

- 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).

This Global Audit Technology Guide (GTAG) was developed to help internal auditors ask the right questions of the IT activity to assess its change management capability, to assess the overall level of process risk, and to determine whether a more detailed process review may be necessary.

After reading this guide, internal auditors will:

- Have a working knowledge of IT change management processes.
- Be able to quickly distinguish effective change management processes from ineffective ones.
- Be able to quickly recognize 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 ensure adequate management supervision.
- Be in a position to recommend the best known practices for addressing these issues, both for assurance of risks (including controls attestations), as well as increasing effectiveness and efficiency.
- Be able to sell recommendations more effectively to the chief information officer (CIO), chief executive officer (CEO), and/or chief financial officer (CFO).

Introduction

This GTAG tackles IT change and patch management as a management tool and addresses:

- Why IT change and patch management are important.
- How IT change and patch management help control IT risks and costs.
- How metrics and indicators can identify what works and what does not work in the change process.
- How to know whether IT change and patch management are working.
- How to reduce IT change risks.
- Internal audit's responsibilities.

The term *board* is used in this GTAG as defined in the *International Standards for the Professional Practice of Internal Audit* (*Standards*) glossary: "a board is an organization's governing body, such as a board of directors, supervisory board, head of an agency or legislative body, board of governors or trustees of a nonprofit organization, or any other designated body of the organization, including the audit committee to whom the chief audit executive may functionally report."

Why IT Change and Patch Management Are Important

Recent research has demonstrated that poor IT change and patch management increase downtime and costs. Over the years, IT activities in various organizations have seen minor changes cause major and prolonged downtime. Where does one 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, in various countries there is specific legislation that requires 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 regulation requirements and affirm the integrity of financial statements.

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 appropriate IT change and patch management can reduce costs.

Without adequate control and visibility, an organization can spend money and effort on unnecessary 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 appropriate 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.

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 it is being changed, and when it is being changed.
- How efficiently and effectively changes are implemented.
- Problems that are caused by changes and the severity of the problems.
- Cost of the changes.
- 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, brake 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.

How to Know Whether IT Change and Patch Management Are Working

As a rough guide, management (including IT management) can understand whether change and patch management are working by asking 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 are they just being evaluated and deferred until "firefighting" 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 the outage was caused by a change? 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?

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***

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 that halts execution of critical business processes, such as coordinating schedules with suppliers and responding to customer orders.
- Downtime on critical applications, databases, or Web servers that prevent users from performing their critical tasks.
- Negative publicity and unwanted board attention.

At an organizational level, indicators that IT activities 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.

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.

How to Reduce IT Change Risks

This GTAG has framed the observed best known practices of change management processes that reduce business risk and increase IT efficiency and effectiveness. In summary, there are five prescriptive steps that organizations can take immediately to improve change management processes:

- Create tone at the top motivating the need for a culture of change management across the enterprise that is 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 the 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 typically 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.

What Internal Audit Should Do

This GTAG discusses 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 performed well, can cause damage to the entire enterprise. This enterprise-wide impact makes it of interest to many boards and, as a result, to top management.

This guide provides tools to help internal auditors obtain and evaluate evidence that IT management's assertions (e.g., performance, effectiveness, and efficiency) are accurate. Mirroring the process of a financial audit,[1] 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, and system outages). 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 audit can assist management and the board by:

- Understanding the organization's objectives regarding confidentiality, integrity, and availability of IT processing.
- Assisting in identifying risks that could arise from changes and determining whether such risks are consistent with the organization's risk appetite and tolerances.
- Assisting in deciding an appropriate portfolio of risk management responses.
- Looking for and fostering a culture of disciplined change management, including promoting the benefits of good change management.
- Understanding the controls that are crucial to a solid IT change management approach:
  - Preventive.

[1] Vincent M. O'Reilly et al., "Overview of Auditing," in Montgomery's Auditing: 12th Edition (New Jersey: John Wiley & Sons Inc., 1998).

    * 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.
- Keeping up to date on leading IT change and patch management processes and recommending that the organization adopt them.
- Demonstrating how management can reap the benefits of better risk management, greater effectiveness, and lower costs.
- Assisting management in identifying practical, effective approaches to IT change management.

The IIA's Change Management-related Standards and Guidance

The following Institute of Internal Auditors (IIA) guidance describes internal auditors' roles and responsibilities pertaining to change and patch management within an organization:

- Standard 2120: Risk Management
- Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes
- Standard 2130: Control
- Practice Advisory 2130-1: Assessing the Adequacy of Control Processes
- Practice Advisory 2130-A1-1: Information Reliability and Integrity

The following IIA Practice Guides also are available for reference:

- *GTAG 1: IT Controls*
- *GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment*
- *GTAG 9: Identity and Access Management*
- *GTAG 17: IT Governance* (pending publication)
- Practice Guide, Auditing the Control Environment
- Practice Guide, Assessing the Adequacy of Risk Management

Why Should Internal Auditors Care About the Way the Organization Is Managing Change?

Internal auditors and IT professionals have had ample guidance on the disciplines of computer operational change management and change control since the early days of computers. The IIA's landmark publication, *Systems Auditability and Control*, updated in 1994, 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. These efforts show 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 it also offers potential benefits to the business.

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

Auditors are aware of the close relationship between change and risk. IT assets seem to be in a state of constant change. For example, 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 an organization does business are releasing patches regularly to repair critical flaws? The volume of urgent patches to be applied to the operational infrastructure and the absence of management process for handling these patches is a critical issue for most organizations.

In low-performing organizations, patch deployment is often characterized as ad hoc, chaotic, and urgent. The availability of a patch to address 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 deployment of the patch can cause unintended problems, such as servers becoming nonfunctional and, therefore, unavailable to deliver critical services.

High-performing organizations are more likely to treat a new patch as a predictable and planned change subject to the normal change management process. The patch is added to the 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. 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.

For the duration of this GTAG, patches are treated as a category or class of change that is 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 that the technologies used to address the "patch-and-pray" problem do not create additional problems.

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 (e.g., 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, an 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.

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. The IT department should publish a change schedule, which lists all approved changes as well as the planned implementation dates. Effective change management processes provide the information and assurance needed to keep track of all changes in the 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.

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 change management process is to sustain and improve organizational operations. This is accomplished by ensuring that 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 (e.g., software, hardware, and information) supporting the organization's critical business processes and data repositories.

Strong change management processes also can 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 compliance. Sarbanes-Oxley Section 404 requires management 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 should be reported to the organization's board. More serious deficiencies, called "material weaknesses" in the public accounting industry, are required to be disclosed publicly by companies through U.S. Securities and Exchange Commission (SEC) filings. Public disclosure of deficiencies could impact the organization's reputation, stock price, and ability to stay in business.

Usually, deficiencies noted in general computer controls, such as change management, are evaluated in relation to their effect on application controls. Specifically, the IT general control (ITGC) weakness is classified as a "significant deficiency" or "material weakness" if one or more of these situations exist[2]:

- An application control weakness caused by, or related to an ITGC, 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 a reasonable period of time.

In previous years, 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 ensure they are corrected in a timely manner.

One model that is generally accepted for assessing internal controls is the 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 revised 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, provides four categories of organizational objectives and eight interrelated components of effective risk management.

High-performing organizations generally have a positive outlook on controls. For example, 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 organization has a more satisfied board, and there is a reduction in pressure on IT department management. 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.

[2] BDO Seidman LLP, et al. "A Framework for Evaluating Control Exceptions and Deficiencies," version 3 (2004). [Developed by the following nine firms: BDO Seidman LLP, Crowe Chizek and Company LLC, Deloitte & Touche LLP, Ernst & Young LLP, Grant Thornton LLP, Harbinger PLC, KPMG LLP, McGladrey & Pullen LLP, PricewaterhouseCoopers LLP.]

Defining IT Change Management

In most organizations, the IT department has two primary roles: operating and maintaining existing services and commitments and delivering new products and/or services to help the organization 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, audit's role in change management, and metrics that can assist in managing change effectively.

What Is the Scope of Change Management?

This GTAG focuses on IT operational change management beginning when upgrades or updates to IT assets (e.g., infrastructure and 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 this guide, excludes the process of configuration management. As defined by the Information Technology Infrastructure Library (ITIL), configuration management is concerned with "identifying, controlling, maintaining, and verifying the versions of all IT components (e.g., hardware, software, and associated documentation)." However, the change management process must interact with the configuration management process (and companion controls) when changes are made to configurations.

Sources of Change

Virtually every business decision requires change in IT. Factors serving as sources of change that must be addressed and managed effectively in the IT environment include:

- External environment (e.g., competitive market, stakeholders/shareholders, changing risks).
- Regulatory environment.
- Business objectives, goals, strategies, requirements, processes, and shifts in priorities.
- Vendors (e.g., 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.

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:*** antivirus software, firewalls, and intrusion protection/detection systems.
- ***Processes, policies, and procedures.***
- ***Roles/responsibilities:*** authorization, authority to act, and access controls.

Change Management Process

A change management process typically includes:

- Identifying the need for the change.
- Preparing for the change.
  - Documenting the change request in detail.
  - Documenting the change test plan.
  - Documenting a change rollback plan in the event of change failure.
  - Writing a step-by-step procedure that incorporates the change, test plan, and rollback plan.
  - Submitting the change procedure in the form of a change request.
- Developing the business justification and obtaining approvals.
  - Assessing the impact, cost, and benefits associated with the change request.
  - Reviewing and assessing the risks and impacts of the change request, including regulatory impacts.
- Authorizing the change request.
  - Authorizing, rejecting, or requesting additional information about the change request.
  - Prioritizing the change request with respect to others that are pending.
- Scheduling, coordinating, and implementing the change.
  - Scheduling and assigning a change implementer.
  - Scheduling and assigning a change tester.
  - Testing the change in a preproduction environment.

  - Communicating the change to stakeholders who likely will be affected.
  - Approving the change for implementation.
  - Implementing the change as requested.
- Verifying and reviewing the implemented change. (This is an often-overlooked critical step.)
  - 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?
- Backing out the change (if unsuccessful).
- Closing the change request and communicating with the affected parties.
- Making agreed-to changes to the change management process.
- Publishing the change schedule.

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 and change authorization, as well as supervision and enforcement. However, to effectively monitor and enforce the process, 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 and thereby reducing repair time.

What Does Ineffective Change Management Look Like?

How does one 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 organization is unable to consistently deploy planned new products and services. 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 (e.g., people and capital), and unbudgeted work.
- Development projects are late and often over budget, which results in late and more costly products and services when compared to 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 switch easily 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, therefore, are implemented poorly or inadequately.
- 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, which results 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.
- Several unauthorized, failed, or emergency patching changes occur.
- Patching systems causes large disruptions due to failed changes that result 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 (e.g., time, resources, and capital) are spent on correcting unauthorized project activities or infrastructure, which takes 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" among 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.

- There is an inability to track changes, report on change status and costs, and there are unauthorized changes.
- Increasingly resources are 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 (e.g., R&D, application developers, auditing, security, and operations) create barriers and introduce unnecessary delays.
- Numerous undocumented changes happening over time increase configuration production variance, which causes lower change success rates and increases the difficulty of deploying patches without failed changes and unplanned work.

What Does Effective Change Management Look Like?

How does one recognize effective change management? Is it possible to walk into an organization and determine whether it has an effective change management process?

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

At the market level:

- The organization 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 generally are 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 change.
- Because of the foundational nature of change management, ensuring compliance with new regulations requires less effort. Virtually every regulation has IT requirements. When controls are well documented, complying with a new regulation is not a new project; rather, it merely becomes 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.
- Resources (e.g., time, effort, dollars, and capital) are applied to implement selected changes with little or no wasted effort (i.e., high change success rate); resources rarely are diverted to unplanned work.
- The organization can confidently answer:
  - "Am I doing the right things?" (an ability to select and prioritize)
  - "Am I doing things right?" (with acceptable quality and performance)
- An effective change management process is demonstrated 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 insecure 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 and require little to no additional information from IT management.
- Variances in production configurations are detected early to incur the lowest cost and least impact.
- The enterprise regularly demonstrates operational excellence with respect to change management.
- Higher service levels (e.g., high availability/uptime/mean time between failures; low mean time to detect problems/incidents; and low mean time to repair) occur in the presence of well-defined processes that introduce planned, predictable change.
- IT is able to quickly return to a known, reliable, trusted operational state when problems arise with a new change or configuration.
- IT demonstrates unusually efficient cost structures (e.g., server-to-system administrator ratios of 100:1 or greater compared with at least one order of magnitude less in low-performing organizations).
- IT is able to identify and resolve operational problems timely, 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, which allows for easier and more accurate reporting to auditors and requires 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.

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 Metrics

Metric and Indicator	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 (i.e., up, down, or steady) should make sense in the business contract.
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.
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.	Higher is better. When changes are not managed and not adequately tested, change success rates typically are around 70 percent. High-performing organizations not only regularly achieve change success rates of 99 percent but also failed changes rarely cause service interruptions or unplanned work.
Number of emergency changes (including patches) is determined by counting the number of changes that required an urgent approval during the week using the change review board or emergency change process.	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. 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.
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.	Higher is typically better. Paradoxically, high-performing IT organizations often have the lowest rate of patching. Some high performers choose to patch annually, despite making thousands of changes every week. They often mitigate vulnerability risks without requiring changes to production systems (e.g., blocking the vulnerability at a firewall).
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.	Lower is better (e.g., 5 percent or less).
Percentage of projects delivered later than planned even though poor project management also may impact this metric.	Lower is typically better. When organizations are spending all their time on unplanned work, there often is not enough time to spend on planned work, such as new projects and services, thereby causing project results to be delivered late.

Figure 1: Unplanned Work as Indicator of Effective Change Management Process

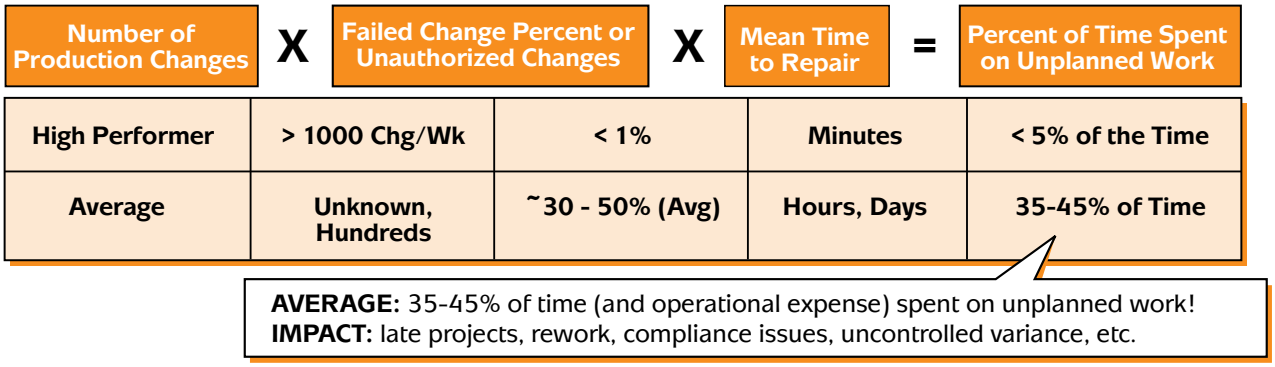
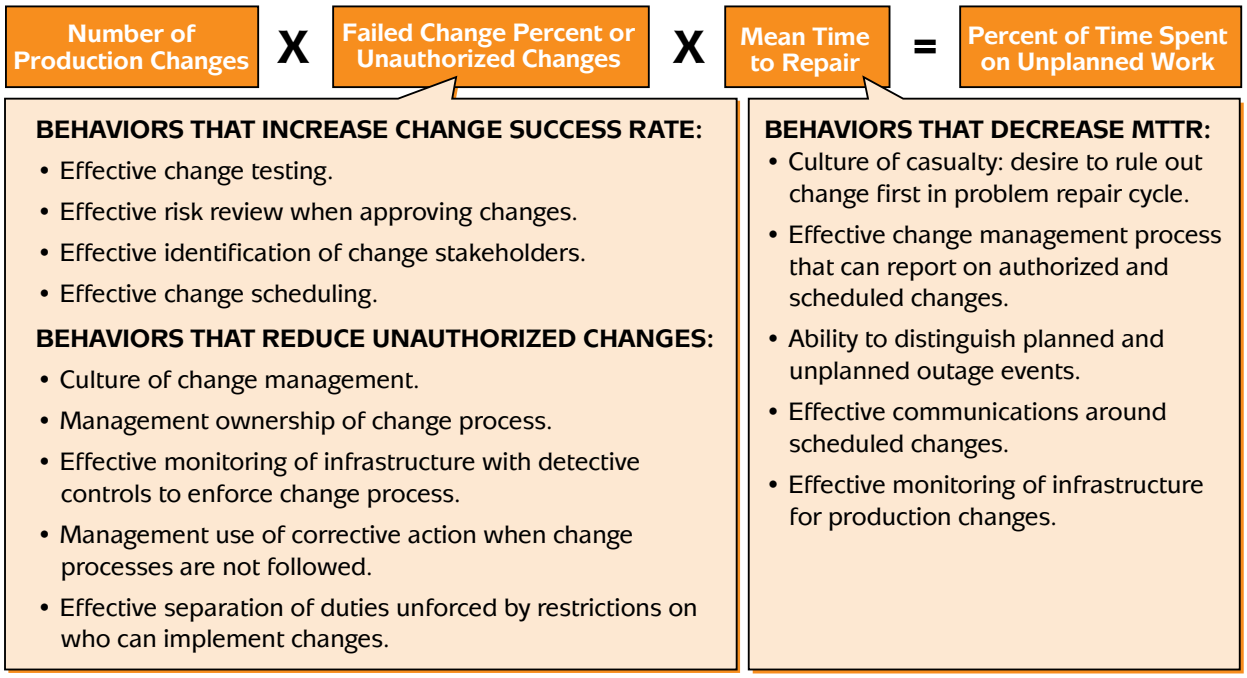


Figure 2: Key Variables That Influence Change Management Processes



Figures 1 and 2 show the key indicators of effective change management and the dominant controls that raise and lower them. The key indicators[3] 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, the result is unplanned work.

This is an extremely simple model and is not intended to be mathematically correct. Rather, 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 (e.g., inadequate preventive and detective controls), unauthorized and failed changes cause protracted outages, which increase unplanned work.

[3] Based on ITPI benchmarking that studied 11 high performing IT organizations and surveyed hundreds of others.

- When IT organizations have a high ratio of unplanned to planned work, they have less time available to do the work 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.

Integrating Patch Management Into Change Management

Despite the urgency attached to applying software patches, patch deployment ideally belongs in preproduction 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 affect many critical systems libraries and 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 and, therefore, require 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 seems to achieve the objective of creating an available and secure computing platform. As previously described, high-performing IT organizations patch far less frequently than typical IT organizations, 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. They also create a release schedule that bundles patches and updates into releases instead of applying individual patches to individual systems.

The risks associated with change are not restricted to applying patches and can be generalized to any automated change deployment technology.

The simultaneous use of patch management and change deployment technologies 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:

- Additional preventive controls to reduce the likelihood of unauthorized changes.
- Independent detective controls to simplify the monitoring, reconciliation, and reporting functions.

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:

- 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 also 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 does one ensure 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 on? Are reports showing the effect of preventive and detective controls easily accessible to management and auditors? When monitoring and reporting controls are functioning properly, IT management has the information it needs to identify issues more effectively and efficiently and is more likely to achieve its business objectives.

What Questions Should Internal Auditors Ask About Change and Patch Management?

This section offers a set of questions auditors may use to get a sense of how effectively changes are managed. The goal 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 managers with an effective change management process.
- IT managers with an ineffective change management process but who are working on improvement (in "problem-solving mode").
- IT managers 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 internal audit. 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."

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
"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 firefighters. We have substantially improved our performance, uptime, and satisfaction from our business customers to our internal staff and all the way up to the 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 on to the production servers."	"We found that one of our vendors was doing some maintenance and updated some software. The 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 on 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."

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
"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."

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 typical stages of change management include:

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."

Where Should Internal Auditors Begin?

According to COSO's 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 organization'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. Internal Audit 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 to ensure IT can recover quickly when changes fail.

Preventive, detective, and corrective controls should be derived from management's objectives for managing IT changes.

To be successful, management must be aligned with the shareholders' concerns 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 — should be achieved. Plans to get to the targets should be formulated and rolled out effectively across the entire organization to have a chance for success. The board wants to ensure that management has identified and assessed the risks that could impede achievement of the objectives. Robust processes should be in place to mitigate, manage, accept, or transfer the risks effectively. Variation from the plan is also a risk that should 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 organizations, 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 risks be managed if their causes have not been identified and analyzed?

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.

Audit's Role in the Change Management Process

Since internal auditors typically do not have time to review every facet of the organizations within which they work, they should develop their audit plans based on a risk assessment. To assist in assessing business risk within IT, auditors should gather preliminary information. 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, auditors should:

- 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 GTAG provides auditors with sufficient background to ask the tough questions of the IT activity to understand the level of improvement that may be needed in its change management process and controls. (Table 2 presents useful questions to ask IT management.)
- Use the indicators of effective and ineffective change management processes to assess the relative effectiveness of the organization's change management 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 it meets the needs of the business.
- 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.)
- 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?

- Perform a brief review to determine whether there are audit trails of changes to the production environment and that the audit trails cannot be manipulated or destroyed.
- When performing change control audits, look for indicators of effective change management. Focus on the risks to the business resulting from the failure to achieve the control objectives.
- Assist management in identifying models with which to improve their approach to change management.
- When the organization is considering outsourcing IT activities to a service provider, verify that the organization's expectations are identified clearly in service level agreements (SLAs) and contracts. Regarding the change management process, it is important to consider:
  - Who is responsible internally for managing day-to-day changes arising from requests to make changes.
  - How the organization knows when the service provider makes changes outside the agreed-upon change management process.
  - What control the organization has 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 implementing changes outside the required change window time periods, with a consequent impact on service (e.g., applications not available when needed) and cost (or loss of revenue)?
  - Who is responsible for ensuring that major business changes affecting IT are properly calculated, approved, planned, controlled, implemented, and periodically reviewed.
  - Whether the provider has considered the impacts on infrastructure (system and network) and information security as part of evaluating each change.
  - Whether the organization identified whom 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.
- 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.

Authors:

Sajay Rai, CPA, CISSP, CISM

Gregory Wilson, CISSP, CISM, CGEIT

Duy Nguyen

Reviewers:

Philip Chukwuma, CISSP

Steve Hunt, CIA

Steve Jameson, CIA, CCSA, CFSA, CRMA

Appendix A: Example Business Case for Change Management

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 internal audit 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 3 summarizes indicators of ineffective change management. Table 4 describes ways in which to address these based on actual field experience.

Table 3: 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."	Poor service levels and availability. Unknown number of operational changes. Uncontrolled rate of change. Low changes success rates (less than 70 percent). High amounts of unplanned work.
"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."	When changes fail, investigating causes and problem management consumed more than 25 percent of the workload. Inaccurate diagnosis leads to poor first-fix rate (less than 50 percent).
"It was like the Wild West. People were not documenting their changes — let alone getting approval. You could tell from our availability statistics!"	Absence of detective controls around change management processes leads to poor performance. Absence of change controls prevents proof of preventive and detective controls for auditors to attest that controls are effective.

Table 4: 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 strengthen the process. We also monitor to ensure that the change management process is being followed."	Increased management visibility of proposed changes. Operational changes are only those authorized by the change management process. Increased control of change rate can lead to change success rate increases to >95 percent due to visibility and testing.
"We started to create real accountability for everyone to follow the change management process. We chose our daily availability management meetings ('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 rogue changes happen much less often!"	(This particular business calculates downtime cost at US $7,000 per minute.) 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 were averted. All changes are fully documented, allowing changes to be ruled out first in the problem repair cycle and restoration time to go from "hours" to "minutes." For the 11 outages in Q3, this saved about 13 hours of system downtime.

Our Remedy	Benefits
"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. "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! "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."	Regulatory compliance is now handled as a day-to-day matter rather than last-minute crash preparation. Because proof of effective change controls is being generated regularly, the external auditors did not generate management comment letters. (Compared to last year, they averted the 130 work hours of unplanned work and audit fees). Mapping change controls to common regulatory requirements reduces the amount of duplicate work done by separate teams. Twelve IT staff members have been reassigned to the IT operations team.
"In addition to all of us not having to wear pagers at home, we're finding that we have much more time to work on planned projects, as opposed to firefighting all the time."	Unplanned work reduced from more than 40 percent to 15 percent. On-time project deliveries went from 0 to 60 percent. The CIO has tasked the IT management group with the key strategic projects for the following year.

Appendix B: Sample Audit Program

Control Objective	Risk	Control	Work Steps
Change Management Process			
To communicate process objectives, requirements and roles and responsibilities.	Errors are made due to lack of understanding of the process.	The change management process is defined and communicated to those involved in the process, including employees and service providers.	Determine whether the process is documented and where it is located. Determine how changes to the process are communicated. From discussions with a sample of those involved, assess their understanding of the process objectives and procedures, as well as the importance of their roles in the process. Validate that they have ready access to related documentation and tools.
Segregation of Duties			
To delegate responsibilities such that unintentional or intentional errors will be detected.	Unexpected or adverse results.	At a minimum, separate people perform the responsibilities for change approval and implementation. Ideally, separate people also will perform design and testing of changes.	Validate that changes are reviewed and approved by an appropriate level of management. Validate that those who approve changes do not have access to implement them in the production environment. Determine how changes are tested to ensure they function as intended and do not impair the integrity, availability, or confidentiality of data.

Control Objective	Risk	Control	Work Steps
Change Management Procedures			
To ensure a change meets business needs.	Unexpected or adverse results.	A standard and centralized process exists for processing all changes.	Select a sample of changes and validate that the controls were performed from initiation through implementation of each.
To ensure a change will not negatively impact availability, integrity, and confidentiality of systems and data.		All changes are approved by the appropriate level of management.	
		All changes are categorized and assessed for impact.	
		All changes are successfully tested by IT and business area personnel prior to implementation into production.	
		All changes are scheduled and communicated to those impacted prior to implementation.	
		All changes to production have an associated back-out plan.	
Emergency Changes			
To ensure business needs are met.	Inability to respond effectively to emergency change needs.	Procedures exist to identify, assess, and approve genuine emergency changes.	Select a sample of emergency changes and validate they meet the definition of a genuine emergency change and the proper controls were performed from initiation through implementation for each.
To ensure a change will not negatively impact availability, integrity, and confidentiality of systems and data.	Unexpected or adverse results.	A post-implementation review is conducted to validate that emergency procedures were properly followed and to determine the impact of the change.	

Control Objective	Risk	Control	Work Steps
Monitoring and Reporting			
To ensure the process is functioning as intended and is understood by those involved and impacted.	Unknown issues.	Metrics are collected, analyzed, and reported to management and those involved in the process.	Determine what metrics exist, how they are calculated, and by whom. Identify whom they are reported to. Determine whether the metrics are appropriate, complete, and accurate. Common metrics collected for the change management process include: • Total number of changes for a set period of time. • Changes that were successful. • Changes that failed. • Success or failure of roll-back plans. • Changes that deviated from the defined change management process. • Percentage of emergency changes. • Number of unplanned outages during a set period of time. • Percent of unplanned work of total work performed by IT personnel.

About IPPF

The International Professional Practices Framework (IPPF) is the conceptual framework that organizes authoritative guidance promulgated by The Institute of Internal Auditors. IPPF guidance includes:

Mandatory Guidance

Conformance with the principles set forth in mandatory guidance is required and essential for the professional practice of internal auditing. Mandatory guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The three mandatory elements of the IPPF are the Definition of Internal Auditing, the Code of Ethics, and the *International Standards for the Professional Practice of Internal Auditing (Standards)*.

Element	Definition
Definition	The Definition of Internal Auditing states the fundamental purpose, nature, and scope of internal auditing.
Code of Ethics	The Code of Ethics states the principles and expectations governing behavior of individuals and organizations in the conduct of internal auditing. It describes the minimum requirements for conduct, and behavioral expectations rather than specific activities.
International Standards	*Standards* are principle-focused and provide a framework for performing and promoting internal auditing. The *Standards* are mandatory requirements consisting of: • Statements of basic requirements for the professional practice of internal auditing and for evaluating the effectiveness of its performance. The requirements are internationally applicable at organizational and individual levels. • Interpretations, which clarify terms or concepts within the statements. It is necessary to consider both the statements and their interpretations to understand and apply the *Standards* correctly. The *Standards* employ terms that have been given specific meanings that are included in the Glossary.

Strongly Recommended Guidance

Strongly recommended guidance is endorsed by The IIA through a formal approval processes. It describes practices for effective implementation of The IIA's Definition of Internal Auditing, Code of Ethics, and *Standards*. The three strongly recommended elements of the IPPF are Position Papers, Practice Advisories, and Practice Guides.

Element	Definition
Position Papers	Position Papers assist a wide range of interested parties, including those not in the internal audit profession, in understanding significant governance, risk, or control issues and delineating related roles and responsibilities of internal auditing.
Practice Advisories	Practice Advisories assist internal auditors in applying the Definition of Internal Auditing, the Code of Ethics, and the *Standards* and promoting good practices. Practice Advisories address internal auditing's approach, methodologies, and consideration, but not detail processes or procedures. They include practices relating to: international, country, or industry-specific issues; specific types of engagements; and legal or regulatory issues.
Practice Guides	Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables.

This GTAG is a Practice Guide under IPPF.

For other authoritative guidance materials, please visit www.theiia.org/guidance/.

GTAG®

About the Institute

Established in 1941, The Institute of Internal Auditors (IIA) is an international professional association with global headquarters in Altamonte Springs, Fla., USA. The IIA is the internal audit profession's global voice, recognized authority, acknowledged leader, chief advocate, and principal educator.

About Practice Guides

Practice Guides provide detailed guidance for conducting internal audit activities. They include detailed processes and procedures, such as tools and techniques, programs, and step-by-step approaches, as well as examples of deliverables. Practice Guides are part of The IIA's IPPF. As part of the Strongly Recommended category of guidance, compliance is not mandatory, but it is strongly recommended, and the guidance is endorsed by The IIA through formal review and approval processes.

A Global Technologies Audit Guide (GTAG) is a type of Practice Guide that is written in straightforward business language to address a timely issue related to information technology management, control, or security.

For other authoritative guidance materials provided by The IIA, please visit our website at www.globaliia.org/standards-guidance.

Disclaimer

Copyright

The Institute of Internal Auditors

www.globaliia.org