IT Change Management

3rd Edition

Supplemental Guidance | **Practice Guide**

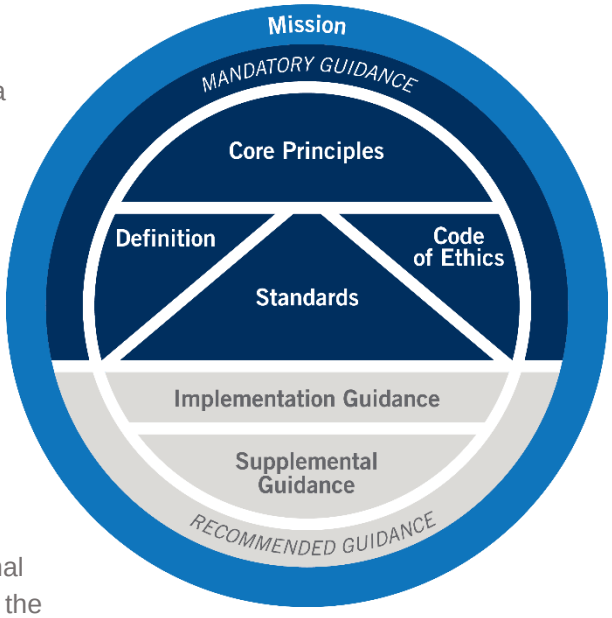
GLOBAL TECHNOLOGY AUDIT GUIDE

The Institute of
Internal Auditors

About the IPPF

The International Professional Practices Framework® (IPPF®) is the conceptual framework that organizes authoritative guidance promulgated by The IIA for internal audit professionals worldwide.

IPPF | International Professional Practices Framework



Mandatory Guidance is developed following an established due diligence process, which includes a period of public exposure for stakeholder input. The mandatory elements of the IPPF are:

- Core Principles for the Professional Practice of Internal Auditing.
- Definition of Internal Auditing.
- Code of Ethics.
- International Standards for the Professional Practice of Internal Auditing.

Recommended Guidance includes Implementation and Supplemental Guidance. Implementation Guidance is designed to help internal auditors understand how to apply and conform with the requirements of Mandatory Guidance.

About Supplemental Guidance

Supplemental Guidance provides additional information, advice, and best practices for providing internal audit services. It supports the *Standards* by addressing topical areas and sector-specific issues in more detail than Implementation Guidance and is endorsed by The IIA through formal review and approval processes.

Practice Guides

Practice Guides, a type of Supplemental Guidance, provide detailed approaches, step-by-step processes, and examples intended to support all internal auditors. Select Practice Guides focus on:

- Financial Services.
- Public Sector.
- Information Technology (GTAG®).

For an overview of authoritative guidance materials provided by The IIA, please visit www.theiia.org.

Contents

Executive Summary

IT change management can be a difficult and complex process to implement and maintain. It requires collaboration among cross-functional teams throughout an organization, and its success or failure can have a significant impact on an organization's operations. As technology advances and organizations move from manual to automated and digital processes and cloud applications, the number of processes subject to change management will only increase. In addition, the need for these systems to function properly and with appropriate and effective controls will be of utmost importance.

Note

The cover, logo, and references in this guide have been updated. The content has not changed.

Throughout this guide, "change management" is defined broadly as "the technology changes that affect an organization's systems, programs, or applications."

Change management controls are an integral part of an organization's IT general controls (ITGCs), and in most organizations, the question isn't whether a change management process exists; it's whether the process is as effective and efficient as possible and is followed for all changes. Generally, effective change management can assist an organization in addressing risk, reducing unplanned work, limiting unintended results, and ultimately improving the quality of service for internal and external customers

Responsibility for change management is no longer the responsibility of IT management only. An organization's entire senior management team should be accountable for managing their risks to levels that enable the achievement of their objectives; and the organization's board, in turn, is responsible for holding management accountable.

The internal audit activity is in a unique position to help senior management and the board recognize the importance of implementing or strengthening their change management program and to help organizations assess and improve their governance, risk management, and control processes related to change management.

This Global Audit Technology Guide (GTAG) will help readers understand the change management process and know the right questions to ask to assess the organization's change management capability. It will help internal auditors assess the overall level of process risk and determine whether a more robust process may be necessary. The guide will also provide an audit approach to assess key areas related to change and patch management.

Introduction

A key aspect of an effective control environment is that an organization has a comprehensive, well-defined combination of controls in place (including preventive, detective, and corrective controls), as well as clearly defined and segregated roles and duties. Change management controls, which include management of patch updates, enable management to address new development projects, regulations, and system changes effectively and efficiently while appropriately utilizing resources.

> **Note**
>
> Terms in bold are defined in Appendix B.

Due to their unique role in an organization, internal auditors have an advantage in evaluating processes and controls and may provide assurance and advice that helps the organization enhance its change management process.

This GTAG focuses on the various aspects of the change management process and addresses:

- What change management is and why it is important.
- How effective change management can help control costs and reduce IT risk.
- The definition of patches and their role in the change management process.
- How metrics and other indicators may be used to determine whether the IT change management process works (according to management's definition or expectations).
- The change management cycle.
- Emergency changes.
- The internal audit activity's responsibilities

This GTAG also provides information to help internal auditors understand the growing complexities and importance of change management, recognize best practices, and assess change management controls. The appendices provide tools to help internal auditors obtain and evaluate evidence to support assessments, such as the validation of control design and operational effectiveness, performance, efficiency, and the accuracy of any applicable management's assertions. Foundational tools are also available for organizations that are new to the change management environment or those that wish to revisit or refresh existing processes.

Specifically excluded from this GTAG are the changes that occur during software design and development, including the concepts of the software development life cycle (SDLC), DevOps (DevSecOps), Agile, and waterfall methods, as these are addressed in other IIA guidance. The guide also excludes detailed discussion of the configuration management process.

This guide will briefly explain some of the types of system tools that can assist in the change management process. However, due to the number of tools available and the diversity of their functionality, this guide will not attempt to explore this area in great detail.

After reading this guide, internal auditors will:

- Have a working knowledge of the change management process.
- Be able to distinguish effective change management processes from ineffective ones.
- Be able to recognize indications of potential control issues related to change management in IT environments.
- Understand that effective change management hinges on implementing preventive, detective, and corrective controls, including the appropriate segregation of duties and adequate management supervision.
- Be in a position to recommend the best practices for addressing these issues, both for assurance that controls mitigate risks and for increasing effectiveness and efficiency.

For more information on IT general controls, readers may refer to The IIA's GTAG "Information Technology Risks and Controls."

Business Significance: Risks and Opportunities

What is change management and why is it significant? In the current business environment, a well-thought-out and systematic change management process is no longer optional; rather, it is necessary for an organization to effectively achieve its business objectives.

Change management can be defined as the systematic set of processes that are executed within an organization's IT function to manage enhancements, updates, installations, implementations, incremental fixes, and patches to production systems. The processes may include (but are not limited to):

- Application code revisions.
- System upgrades (e.g., applications, operating systems, and databases).
- Infrastructure changes (e.g., servers, cabling, routers, and firewalls), including on-premise, cloud, and mobile.
- Security patches/updates (e.g., correcting known security vulnerabilities in hardware, software, applications, and databases).

Change management can also be described as a consistent and understood process to minimize disruption while modifying the IT environment.

- Addition or deletion of hardware and software.
- Code modifications or revisions.
- Configuration changes to existing hardware.
- Regular system updates or patches.
- Data modifications (e.g., restoring from backup).

The exact structure of the change management process may differ in every organization, but the goal of change management in an IT environment is to ensure that change requests (including emergency maintenance) are handled quickly, efficiently, and effectively. This goal is accomplished by following consistent procedures and maintaining them in a controlled manner. This systematic approach improves business operations by reducing the potential of issues related to confidentiality, integrity, or availability.

Properly implemented, change management protects the production environment ("live" environment) and provides the organization with a repeatable, measurable, and auditable process that captures all technology-related changes.

Patches as Part of the Change-Management Process

Patches are changes to a computer program designed to address a security vulnerability, an operational deficiency, or to add new or upgraded features between software releases. They may repair vulnerabilities or other defective code unintentionally occurring in the production environment.

Typically, software vendors notify users of pending changes, and it is incumbent on those users to incorporate patches into the change management process with as little organizational disruption as possible. However, many vendors now “push” or automatically (and proactively) implement patches without requiring or involving an organizational request, initiation, or other intervention.

In the context of this document, patches are treated as a category or class of change that is subject to the company’s normal change management process.

Risks Related to Change Management

General Risks

A poor change management program may expose the organization to many risks, including unauthorized or unrecorded changes being applied, system or application failure/downtime, security issues, inefficient business processes, inconsistent results, and even misstated reports and financial statements

In addition, inefficient or ineffective change management can cost an organization through:

- Failure to achieve business objectives.
- Control deficiencies that may result in inconsistent compliance or negative audit results.
- Attrition of highly qualified IT staff due to frustration over low-quality results.
- Poor quality systems that can hinder employee productivity or frustrate customers.
- Missed opportunities to provide innovative or more efficient products and services to customers.
- Outages and unplanned work.
- Failure to conduct a threat analysis or test and implement necessary patches, which can introduce new critical security vulnerabilities or reintroduce prior vulnerabilities.
- Failure to properly engage the organization in the change advisory board (CAB)/change approval process, which increases the chance that change could impact the completion of a critical business activity.
- System changes that do not meet process owner needs, resulting in processing errors, lost time due to rework, and other negative outcomes.
- Slow information processing or instability in system operations.

Patch-related Risks

Patches tend to affect many critical systems libraries and other software used by application programs. Patches can be large and/or complex changes, and often are intended to correct

critical vulnerabilities. In addition, documentation of the change may be limited. Even small configuration variances may cause drastically different outcomes.

Further, as mentioned, patches are often pushed by vendors automatically and could potentially occur outside of the change schedule. Although this can be a convenience, it can also introduce additional risks. IT personnel should not only be aware of the timing for patches being pushed to allow for appropriate preparation but should also understand the implications a patch may have across the organization.

These factors can potentially affect the change success rate and may require more comprehensive planning, execution, and testing.

Emerging Risks

As the global community embarks on what is referred to as the fourth industrial revolution (e.g., automation, artificial intelligence), potentially profound risks, which may be difficult or impossible to foresee, are emerging.

Many organizations simply focus their change management process on managing changes within their on-premise systems. The scope of the change management process should also consider emerging risks of a more global and cyber nature. Specific considerations include:

- Cloud applications and how changes are applied to those applications that support infrastructure, which are sources of third-party risk.
- Mobile device applications and how changes are applied to the hardware, operating systems, and applications.
- BYOD (“bring your own device”) and whether the changes are managed by an organization or the individual device owners.

End-user Computing and User-developed Applications

Many organizations operate systems that are inherently complex because they involve end-user computing (EUC) or user-developed applications. In these systems, end-users may build their own processing or reporting applications using existing applications and tools such as Excel, Access, SQL, columnar databases, visualization tools, robotic process automation (RPA) tools. Designing comprehensive controls around these systems may be challenging because they are complex and customized.

In addition, some of these projects, which may have previously been adopted as larger scale IT change initiatives, may be overlooked or dismissed due to the smaller magnitude (e.g., less than a certain number of hours) or when weighed against an arbitrary return-on-investment equation. Management and internal auditors should understand these complex systems, including their capacity, capability, and pervasiveness. Users should also be considered. Understanding these factors will help management and internal auditors assess relevant risks and the applicability of the change management controls around these critical processes and systems.

Third party and Compliance Risks

Vendors and Control Reports

With the proliferation of vendor relationships, understanding who is responsible for associated change management controls can be challenging. Vendor offerings range from applications

completely hosted in the cloud to applications in private clouds, completely controlled by the organization.

Many vendors produce a report on their system-level and organizational/entity-level controls, which may offer various levels of assurance. Obtaining and evaluating these reports may be necessary for the organization's regulatory compliance (e.g., Section 404 of the U.S. Sarbanes-Oxley Act of 2002).

However, merely obtaining a vendor's report over their controls does not guarantee those controls are effective. Management should understand how to read the report and its scope. Management should also evaluate whether the vendor's controls are effective. Additionally, management should understand which control responsibilities belong to the vendor and which belong to the organization (the latter are known as Complementary User Entity Controls [CUEC] or User Control Considerations [UCC]).

In addition, ensuring all contracts with management service and cloud providers include specific language regarding patches and patch deployment notification helps ensure the organization is properly managing change and ultimately managing their data and information assets, whether internally or externally.

Compliance Risks

Strong change management processes can assist an organization in maintaining compliance with new or expanded regulations. Activities that address the potential impact of changes on regulatory compliance should be included within the risk evaluation and business unit approval steps of the change process.

For example, for companies subject to compliance with regulations such as Japan's Financial Instruments and Exchange Act, India's The Companies Act of 2013, or the U.S. Sarbanes-Oxley Act, care should be taken when implementing changes to technology supporting the financial reporting process. Each of these regulations requires various levels of validation and assessment of controls over the financial reporting process, including IT controls. Without effective change management, it may be difficult for management to affirm the integrity of financial statements and meet regulatory requirements.

In addition, according to the United Nations Conference on Trade and Development, 107 countries have enacted some form of legislation to ensure the security and protection of consumer data and privacy.[1] Companies subject to these regulations or overarching regulations, such as the European Union's General Data Protection Regulation (GDPR), should be cautious about changes that may affect personally identifiable information within their systems. Violations of these acts can result in severe and costly penalties.

[1] United Nations Conference on Trade and Development, "Data Protection and Privacy Legislation Worldwide," March 27, 2019. https://unctad.org/en/Pages/DTL/STI_and_ICTs/ICT4D-Legislation/eCom-Data-Protection-Laws.aspx

Change Management Elements, Management's Responsibilities, and Patches

In most organizations, IT has two primary roles: (1) operating and maintaining existing services and commitments and (2) delivering new products and/or services to help the organization achieve its objectives. This section describes the elements of change management that support these two roles, as well as management's controls, the characteristics of effective and ineffective change management, and the concept of patches within the change management process.

Elements of Change Management

Environments and Migration

A recurring theme throughout this document is that change management should facilitate protecting the system's or application's live, production environment. However, systems and applications may have several environments, and there is no universal or correct structure.

Different systems may have different environments, but will typically consist of an initial development environment (DEV) and a production environment (PROD), as well as transitionary environments for processes such as experimenting, testing (TEST), quality control, staging, data migration, and user acceptance testing (UAT). The various environments used by a given application should be as identical as possible regarding hardware, software versions, and patches, and management and the internal audit activity should have a thorough understanding of those environments.

The specific movement of changes from environment to environment is called migration, and an important control in migration is ensuring duties are appropriately segregated. Organizations should apply a risk-based approach to segregating duties related to their change management process, based on their risk appetite and risk profile. When segregation of duties is not feasible or ideal, the organization should ensure appropriate detective or monitoring controls are in place. Figure 1 depicts the migration of a change through different environments with duties segregated.

Figure 1: Example of an IT Change Migration

Note: The migration through each of these environments should be properly segregated.
Source: The Institute of Internal Auditors.

Standardized methods and procedures within a change management structure support effective and efficient handling of changes through each environment and minimize the impact of change-related incidents on service quality and availability. To protect the production environment, changes should be managed in a repeatable, defined, and predictable manner. Care should be taken to ensure changes made to correct one application, server, or network device do not have unintended consequences 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.

Types of Change

Changes may be categorized in many ways, but generally should be grouped together by timing, urgency, and/or levels of perceived risk. In addition to patches, other types of change that may occur include:

- Regular changes – typically application, middleware, operating system, or network software and hardware upgrades scheduled for implementation.
- Emergency changes – to correct immediate issues that cause service disruption.
- Preapproved changes – regularly or frequently occurring, lower risk changes that a CAB or other appropriate approver has authorized for implementation.
- Blanket changes – typically a master ticket is created as needed (e.g., monthly, quarterly) to record a group of changes, such as router configuration changes, firewall rule updates, and sometimes Microsoft monthly patches.
- Automation "bot-driven" changes – processes built into a tool that automatically promote software changes, including patches, from one environment to another without the need for additional human intervention.

Sources of Change

Virtually every business decision will initiate a change in the IT environment. Sources of change that should be addressed and managed effectively include:

- External environment (e.g., competitive market, stakeholders/shareholders, changing risks, geopolitical events).
- Regulatory environment (e.g., developing new reporting capabilities to comply with new or updated regulations).
- Modifications or updates to business risks, objectives, goals, strategies, requirements, processes, and shifts in priorities.
- Upgrades.
- Patches.
- New products, vendors, partners, or suppliers.
- Identified vulnerabilities.
- Results of an audit, risk assessment, and other type of evaluation or assessment.
- Corrections to operational issues.

- Changes in performance or capacity requirements.
- New or retired technology.

Scopes of Change

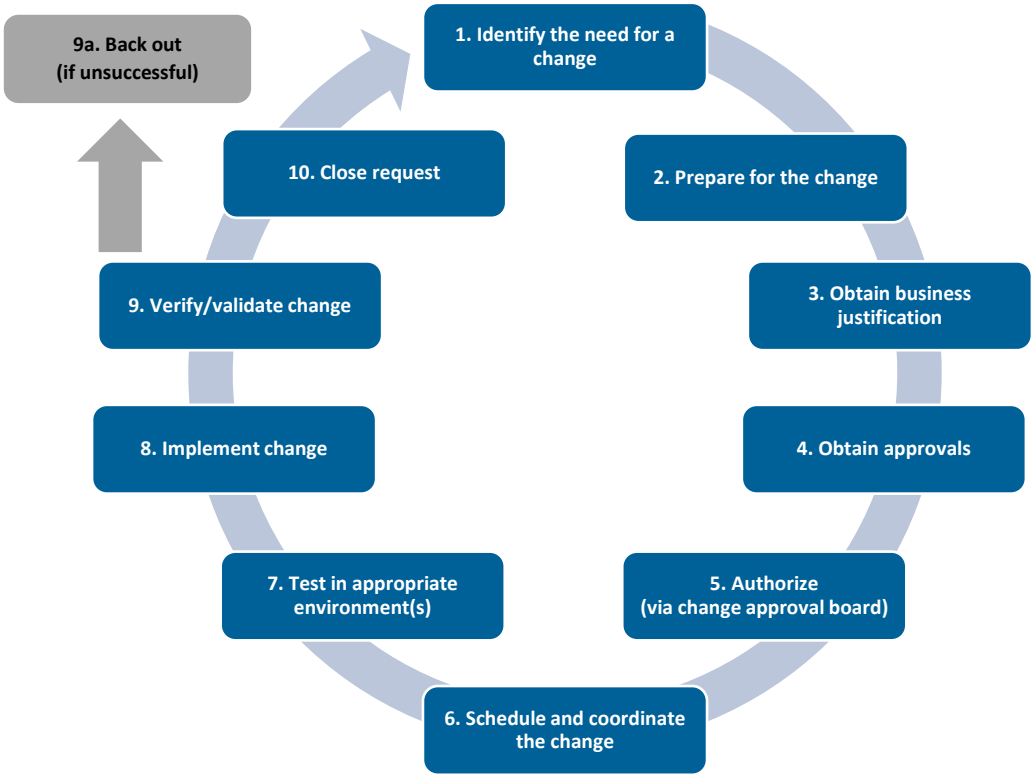
An effective change management process encompasses within its scope any alterations to IT-based assets on which business services depend. Assets subject to change management include:

- *Hardware* – workstations, laptops, tablets, phones, servers, routers, switches, and core infrastructure components such as power generation or cooling, networked printers, and mobile devices.
- *Software* – operating systems, middleware, and applications (including in-house developed applications and commercial off-the-shelf applications).
- *Information, data, and data structures* – individual file updates, complete database updates (e.g., restoration of a previous version), and data integration jobs.
- *Security controls* – antivirus software, firewalls (both installation of new equipment and of rules), and intrusion protection/detection systems.

Process Steps

Figure 2 shows likely steps in a change process. However, process steps will differ among organizations, and some steps may occur concurrently. Appendix C describes a more detailed change management process.

Figure 2: Sample Steps in a Change Process



Source: The Institute of Internal Auditors

Scheduling

To assess and report the status of changes continually, management should publish a change schedule that lists all approved changes as well as planned implementation dates. In alignment with the organization's change management process, proposed changes should go before a CAB comprising business and IT leaders from the organization. Once the changes have been approved, an implementation schedule should be created, published, and updated regularly. This process helps provide the information and assurance required to track all changes in their various states of completion.

Change Management Tools

Although this document will not go into in-depth details, there are numerous software and process tools available to facilitate and assist in the change management process. Types of tools include but are not limited to:

- Ticketing systems – often categorized as services management tools. Most have modules for change, problem, release, knowledge, asset, and configuration management. Organizations that implement all modules can use the tool to manage their assets from beginning to end.
- Code repositories – allows organizations to manage software updates. Code is stored in a securely located repository that requires programmers to check out code they are tasked with changing. Once changes are complete, the code is checked back in. This method ensures documentation and version control.

- Orchestration change tools – these perform functions including code promotion between environments, server provisioning, and automated patch deployment.

When selecting and using a tool to assist in the change management process, management should understand the capabilities, functionalities, and limitations of each tool. Risks are commonly introduced when multiple tools are used with multiple interfaces, separate tools are used for different types of changes, and tools are managed across diverse and/or multiple geographic locations

Continuous Evaluation and Improvement

Change management is an evolutionary process, and each organization's progression along the spectrum of maturity is unique. Many factors affect the organization's position, trajectory, and rate of progress. Organizations should evaluate and improve change management processes on a consistent basis to keep up with technology and the global environment as much as possible.

Care should be taken, however, when introducing a new change management program or updating an existing one. Changes that are poorly designed and implemented may result in unnecessary expenditures and unplanned/emergency work to minimize any negative impacts. Progressing to another maturity level is less important than the quality and integrity of the process to get there.

Management's Controls

Effective change management requires proper governance (including IT governance), which includes developing, documenting, and enforcing change policies and ensuring employees are continually trained. It also includes controls to ensure all changes are authorized and auditable and that unauthorized changes are investigated.

Preventive controls include segregation of roles/duties and change authorization. In addition, detective controls should be in place to effectively monitor the production environment for changes, to reconcile these changes to approvals, and report unauthorized variances. Change management controls can also be corrective during outages and service impairments, allowing change to be ruled out first in the repair cycle and thereby reducing repair time.

Effective Change Management

Change management has an impact on the entire organization, and therefore management should be aware of the positive and negative effects that can occur when designing and implementing a strategy. To be effective, change management processes should cover:

- What is being changed, why it is being changed, and when it is being changed.
- Whether the change is properly authorized based on specific criteria.
- Who requested the change.
- Who is responsible for performing the change.
- Who is responsible for validating the change.
- How efficiently and effectively changes are implemented.

- Potential unintended outcomes/problems that may be caused by change, the impact of those outcomes/problems, and remediation plans.
- The cost and benefits of the change.

This information should be reported to senior management regularly and objectively using metrics and indicators, for example, in dashboard-type reports. Such reports allow senior management to gauge IT's progress toward:

- Aligning end-users with IT changes to meet business needs.
- Creating defined, predictable, and repeatable processes with defined, predictable, and repeatable results.
- Coordinating and communicating with stakeholders affected by changes.

In addition, more rigorous, formal measures and specific metrics should be reported to provide maximum visibility into the impact of the strategy on the effectiveness of IT change management. Indicators may include:

- Number of changes authorized over a specific period.
- Number of changes implemented over a specific period.
- Number of unauthorized changes that circumvent the documented change process.
- Change success rate (percentage of changes made that did not cause outages, service impairments, or an occurrence of unplanned work).
- Number of emergency changes (including patches).
- Average duration from patch release date until patch is deployed to vulnerable IT systems.
- Percentage of time spent on unplanned work.
- Percentage of projects delivered later than planned.

Analyzing the results may indicate whether the organization has an effective change management process, whether the process benefits the business, and where to focus more resources.

Appendix D lists sample questions to assess effective change management.

Results of Effective Change Management Processes

Organizations with effective change management require fewer system administrators and typically have increased effectiveness and productivity of IT personnel. When change management is operating effectively, IT personnel are better equipped to:

- Upgrade software and applications regularly, improving the overall security and functionality of systems.
- Update systems in compliance with regulatory standards.
- Protect systems from cybersecurity incidents.
- Operate in a continuous integration/continuous deployment environment.

- Allocate more resources on initiatives that help achieve business goals and fewer on unplanned work.
- Reduce system vulnerability and experience less downtime.
- Install patches with minimum disruption.
- Be proactive and focus on improvements rather than "putting out fires."
- Ensure scripts/bots are operating effectively and monitored properly.

Quite simply, if the change management process is effective, the organization may realize significant cost savings.

High-performing organizations generally have a positive outlook on controls. For example, effective change management processes may result in fewer issues being highlighted by external auditors, regulators, or equivalent authorities. As a result, the organization may have a more satisfied board, resulting in less pressure on IT management and ultimately a more satisfied staff and lower turnover.

Change management hinges on processes with a managerial and human focus, supported by technical and automated controls. Ultimately, organizations that treat change management controls as enablers for effective business conduct are more successful. Employees have access to better tools to boost productivity, and customers enjoy systems that meet their needs.

Benchmarking Effective Change Management

Indicators of effective change management may appear as a feature of maturity (e.g., predictable, repeatable, managed, measurable, and measured). Appendix E, "Characteristics of Effective and Ineffective Change Management Processes," explores these maturity indicators as they relate to several organizational dimensions, including market, client/customer/stakeholder, enterprise, and IT infrastructure.

Patches

As previously described, patches are changes to a computer program designed to address a security vulnerability or an operational deficiency or to add new features between releases. Typically, vendors of commercially available software announce patches on their websites. Additionally, patches correcting security vulnerabilities can be found on both the United States Department of Homeland Security website and on the National Vulnerabilities Database (NVD).[2,3]

An organization may deploy patches manually or through a patch deployment or orchestration tool and/or by one or more third parties. Organizations should ensure contracts with third parties adequately address patch management, including patch-related communication, and are tied to service-level agreements (SLAs).

Despite the potential urgency attached to applying software patches, patch deployment ideally belongs in preproduction processes where patches can be tested adequately in a staging or "sandbox" environment. Ideally, patches are deployed as part of a scheduled patch management

[2] CISA Cyber+Infrastructure, Department of Homeland Security, us-cert.gov, accessed on January 7, 2020.
[3] National Vulnerability Database, NIST, https://nvd.nist.gov/.

cycle, but this is not always the case. When organizations work with vendors that automatically push patches, IT management should take steps to be aware of the timing of the automatic implementation.

Assessing Patch Risks

Unmitigated security vulnerabilities may expose IT assets to significant risk. To properly protect IT assets, patching must occur timely. The organization should regularly perform risk assessments that consider the impact and likelihood of risks that could occur due to untimely or insufficient patch application.

Patch Schedule

Applying patches in a timely manner (once released by a vendor) is key to avoiding risks posed to an organization's system and its critical data. Organizations that have a well-defined and understood patching process will be more efficient and timely in applying patches. An effective patching process should include a patch release schedule of major vendors, a way to be aware of vendor pushes, clear roles and guidelines to prioritize security vulnerabilities, and defined acceptable timeframes to apply patches as informed by a risk assessment.

Organizations should create a schedule that bundles patches and updates into releases rather than applying individual patches to individual systems. The simultaneous use of patch management and change deployment technologies make the process more efficient and effective.

Critical Security and Functionality Patches

Many cybersecurity incidents occur due to vulnerabilities that could have been prevented or remediated by existing patches that had not yet been applied. For example, in the 2018 Equifax data breach, a failure to patch a critical system led to the compromise of personally identifiable information (PII) of 148 million consumers. A report from the U.S House of Representatives Committee on Oversight and Government Reform stated: "Equifax failed to fully appreciate and mitigate its cybersecurity risks. Had the company taken action to address its observable security issues prior to this cyberattack, the data breach could have been prevented."[4]

The volume of urgent patches to be applied to the operational infrastructure and the absence of management processes for handling these patches can be critical. To ensure the security of existing systems, patches must be applied regularly in all critical applications and devices. Timeframes for the application of patches are often based on the criticality of risk, which should be determined by each organization.

Many IT professionals, especially those in North America, are familiar with "Patch Tuesday," the unofficial term referring to the pattern Microsoft has established of issuing patches. Typically, the second and sometimes the fourth Tuesday of each month, Microsoft releases patches for its software products. There may be in excess of one hundred patches in any given update. Microsoft's releases are not limited to these days, but it has been a relatively standard practice since 2003.

[4] U.S. House of Representatives Committee on Oversight and Government Reform, "The Equifax Data Breach," Majority Staff Report, 115th Congress, December 2018, https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

The National Vulnerability Database assigns a criticality score to each patch from zero to 10. Patches rated 6 to 10 are critical, meaning they are more likely to expose data and information assets and/or are more likely to allow a bad actor to take over an impacted device/system. Management should understand how critical vulnerabilities are discovered and what process is followed to assess, test, and address weaknesses.

Zero-day refers to a vulnerability or weakness in a system has been discovered but the vendor has not yet provided a formal remediation. Organizations should have a plan to address Zero-day vulnerabilities because they may not be able to wait for a patch or other instructions for mitigation. Instead, the organization may need to immediately conduct a high-level threat analysis and implement a compensating control.

For organizations relying on third-party vendors for cloud application services, management should understand the vendor's patch policy and how vendors manage patches. This information is typically found in service organization control (SOC) reports.

Effective Patch Management

The availability of a patch to address a critical security vulnerability can be disruptive and may result in significant resources being redirected from planned work to address the unplanned patch, exposing the organization to security incidents. Worse, even successful deployment of a patch can cause unintended problems, such as servers becoming nonfunctional and unavailable to deliver critical services.

Organizations with effective patching functions will likely treat a new patch as a predictable and planned change subject to the normal change management process. A new patch is added to the queue to be evaluated, tested, and integrated into an already-scheduled release deployment. Following a well-defined process for integrating patches leads to a much higher change success rate.

The Role of Internal Audit in Change Management

Internal Audit Responsibilities

An efficient and effective change management process is a critical service that helps the organization achieve its objectives. The internal audit activity can validate the existence and adequacy of the change management process and can provide assurance that the controls supporting the process are designed appropriately and operating effectively.

When performing an audit or review of the change management process, internal auditors must "identify sufficient, reliable, relevant, and useful information to achieve the engagement's objectives," according to Standard 2310 – Identifying Information. This could include gathering material on underlying 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 information regarding system outages). By doing so, auditors will have detailed support needed to express an opinion on the design and operating effectiveness and efficiency of the change management process, the organization's ability to mitigate risks in this area, and on any related assertions made by IT management (e.g., performance, effectiveness, and efficiency).

Internal auditors must develop and document a plan and establish objectives for each engagement. In addition, the established scope must be sufficient to achieve the objectives of the engagement. The requirements are described in Standards 2200 – Engagement Planning, 2210 – Engagement Objectives, and 2220 – Engagement Scope.

Internal auditors should independently corroborate that management has identified risks that could arise from changes and assist in determining whether such risks are consistent with the organization's risk appetite and tolerances. Internal auditors can also determine whether a culture of disciplined change management exists, and can promote the benefits of good change management protocols to key stakeholders.

To conform with the Competency principle of The IIA's Code of Ethics and Standard 1210 – Proficiency, the internal audit activity collectively must possess (or obtain) and apply the knowledge, skills, experience, and other competencies needed to perform its responsibilities. Further, internal auditors must have sufficient knowledge of key IT risks and controls and available technology-based audit techniques to perform their assigned work.

Additionally, when assigning auditors to an engagement that may require specific skills and abilities, Standard 2230 – Engagement Resource Allocation states, "Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives based on an evaluation of the nature and complexity of each engagement, time constraints, and available resources." The interpretation of that standard indicates: "Appropriate refers to the mix of

knowledge, skills, and other competencies needed to perform the engagement. Sufficient refers to the quantity of resources needed to accomplish the engagement with due professional care."

Standard 2340 – Engagement Supervision states: "Engagements must be properly supervised to ensure objectives are achieved, quality is assured, and staff is developed." If an internal audit activity lacks personnel with the skills necessary to provide assurance over the change management process, the chief audit executive (CAE) must obtain competent advice and assistance and may choose to outsource or cosource the engagement. When outsourcing, the CAE retains overall responsibility for supervising the engagement and for reviewing and approving the final engagement communication (Standard 2440 – Disseminating Results).

Overarching areas in which internal auditors can provide organizational value include:

- Keeping current on leading IT change and patch management processes and recommending that the organization adopt those that apply.
- Demonstrating how effective change management can help the company reap the benefits of better risk management, greater effectiveness, and lower costs.
- Assisting management in identifying practical, effective approaches to change management.
- Participating as nonvoting members of the change advisory board.
- Understanding the process followed by the organization to keep current on patch availability as well as the deployment practices in place.

Understanding and Assessing the Change Management Process

Internal auditors, together with management, want to ensure risks have been identified and are being mitigated or managed properly. While IT management's responsibility is to protect the production environment and support the organization's pursuit of its business objectives, internal auditors should assess and validate that appropriate risk management processes and controls are in place.

Engagement Timing and Scope

The timing and frequency of change management engagements may be regulated, but even when they are not mandated, internal auditors should consider conducting reviews on a regular basis, based on risk. The review of an organization's change management process can be a stand-alone assessment, or included as a part of a larger audit, such as a component in the periodic review of the organization's internal controls over financial statements.

Regarding engagement scope, in part, Standard 2220 states that the established scope be sufficient to achieve the objectives of the engagement and include consideration of relevant systems, records, personnel, and physical properties, including those under the control of third parties. The scope of the audit or review can be affected by factors such as but not limited to internal audit staffing, time sensitivity, mitigating processes, prior deficiencies, and newly identified risks.

Planning Considerations

Planning considerations should include gathering relevant information and understanding the organization's governance structure and the specific strategies, objectives, and risks of the

change management process. Sufficient engagement planning will provide internal auditors with the necessary information and background to develop relevant questions and steps to perform an audit or review of the change management process and controls. Specifically, according to Standard 2201, internal auditors must consider the following:

- The strategies and objectives of the activity being reviewed and the means by which the activity controls its performance.
- The significant risks to the activity's objectives, resources, and operations and the means by which the potential impact of risk is kept to an acceptable level.
- The adequacy and effectiveness of the activity's governance, risk management, and control processes compared to a relevant framework or model.
- The opportunities for making significant improvements to the activity's governance, risk management, and control processes.

Assessing Management's Approach

Management's attitude and approach regarding the importance of change management will have a significant impact on the overall maturity and effectiveness of the program. As a part of planning, and from an overall assessment standpoint, internal auditors should understand management's general outlook and approach regarding change management and determine how these views affect the efficiency and effectiveness of the process.

Assessing the Change Management Process Using a Risk-based Approach

Since internal audit departments typically do not have the resources to review every facet of the organizations in which they work, engagement plans are based on a risk assessment, which helps determine the scope, depth, and magnitude of the review.

Although each audit program will differ, internal auditors should consider performing some of these general steps when conducting an audit or review of an organization's change management and control processes.

- Understand the basic components of change management and its implementation in the organization.
- Perform a walk-through of the change management process, seeking evidence of the key elements outlined in this guide.
- Understand how IT management is measuring the process and whether it meets the needs of the business.
- Determine if management has a method of reporting metrics for process results and effectiveness.
- Determine whether metrics are being used to monitor the process and drive continuous improvement, and whether they are appropriate and effective.
- Determine whether IT management has assigned responsibility for change management to someone other than software developers or others who prepare changes in alignment with appropriate segregation of duties.
- Verify management has secured the production environment so only those responsible for implementing changes can in fact implement changes.

- Determine whether changes to the production environment are documented, auditable, and retained in a way that cannot be manipulated or destroyed (i.e., audit trails).
- Apply data analytics techniques and develop or use indicators of effective and ineffective change management processes to assess the organization's relative effectiveness.

In auditing IT change management processes, internal auditors should at least validate authorization, segregation of duties, testing of changes, approval to move changes into production, and validate emergency changes. These areas may be the most critical and if not properly managed, could expose the organization to the most significant risks.

Specific Change Management Controls

Preventive – controls that deny certain changes unless specific actions or conditions are met, such as:

- Appropriate authorizations, including by the change advisory board when necessary.
- Segregation of roles/duties, including:
    - The physical act of migrating the change should be performed by an employee who is independent of the actual change process. Typically, this is completed by the change and release manager.
    - Implementer did not authorize their own changes. (See additional details in the "Migration and Segregation of Duties" section below.)
- Completion of minimum required steps.
- Appropriate and complete documentation of changes (i.e., description, risk, systems impacted, rollback/backout plan).
- Appropriate permissions are in place.

Detective – controls that monitor completed changes to determine if any undesirable changes or unintended outcomes have occurred. These controls could include:

- Detection of unauthorized or incorrectly authorized changes.
- Monitoring of valid, objective change management metrics.

Corrective – predetermined actions taken when certain post-change conditions or behaviors are found. These controls could include:

- Post-implementation reviews.
- Change information fed into early problem diagnosis steps.

Migration and Segregation of Duties

When evaluating the migration of changes between environments, internal auditors should look for assurance that specific segregation of duties are in place and consistently observed, such as the actual migration of a change being completed by a person who is independent from the development team, as there is a risk that unauthorized changes may be made to production code. In many organizations, the change and release manager performs this function

Internal audit should validate that only authorized personnel can migrate a change into the production environment by checking the security access profiles of users. While conducting this

work, the auditor may review the profiles of developers to ensure their access is restricted to development environments. When duties are not properly segregated, the auditor should then attempt to validate mitigating detective or monitoring controls.

Appendices F and G provide a sample change management audit program and metrics.

Outsourced Function Considerations

Organizations may find it necessary to outsource or cosource some or all of their IT functions, including the change management function. When the organization outsources IT activities to a service provider, internal auditors should verify that the organization's expectations are identified clearly in service-level agreements (SLAs) and contracts. Internal audit also should work with management to ensure "right-to-audit" clauses are included in third-party contracts.

> **Resource**
>
> See IIA Practice Guide "Auditing Third-party Risk Management" for additional information.

Regarding an outsourced change management process, it is important for internal auditors to:

- Determine whether the service provider uses specific privileged user accounts for change purposes, and whether these accounts are tracked and changes recorded/maintained.
- Determine parties responsible for managing day-to-day changes arising from requests to make changes.
- Identify how the organization can detect whether changes are made outside the agreed-upon change management process.
- Determine controls the organization uses to ensure it is not charged for unauthorized or unreasonable changes.
- Determine controls the organization uses to prevent vendors from implementing changes outside the agreed-upon window or timeframe for changes.
- Determine parties responsible for ensuring that major business changes affecting IT are properly calculated, approved, planned, controlled, implemented, and periodically reviewed.
- Determine whether the service provider has considered the impacts on infrastructure (system and network) and information security as part of evaluating each change.
- Determine who monitors compliance with the SLAs.
- Determine if SLAs incorporate required practices, validation procedures, timing of the testing required, remediation work, retesting, and other considerations if the organization is subject to Sarbanes-Oxley Section 404 (or similar regulations over internal controls) and/or requirements of other regulations.

Audit Findings/Observations

When discussing and writing audit observations, internal auditors should present the business value of effective change management processes as well as the risks of ineffective ones. Internal auditors should clearly articulate the operational, financial, and regulatory risks that are not being

managed appropriately, and relate the findings to the risk tolerances management has established in support of its business goals and objectives.

Internal auditors should consult with management throughout the engagement process and obtain management's recognition of any observations (including the severity) and any action plans, before issuing any reports. Standard series 2400 can be used to guide the CAE's communication with senior management and the board.

Additional requirements are described in Standards 2110 – Governance, 2120 – Risk Management, 2130 – Control, and 2330 – Documenting Information.

Appendix A. Relevant IIA Standards and Guidance

The following IIA resources were referenced throughout this practice guide. For more information about applying the *International Standards for the Professional Practice of Internal Auditing*, please refer to The IIA's Implementation Guides.

Code of Ethics
Principle 4 – Competency
Standards
Standard 1210 – Proficiency
Standard 2110 – Governance
Standard 2120 – Risk Management
Standard 2130 – Control
Standard 2200 – Engagement Planning
Standard 2201 – Planning Considerations
Standard 2210 – Engagement Objectives
Standard 2220 – Engagement Scope
Standard 2230 – Engagement Resource Allocation
Standard 2310 – Identifying Information
Standard 2330 – Documenting Information
Standard 2340 – Engagement Supervision
Standard 2400 – Communicating Results
Standard 2440 – Disseminating Results
Guidance
Practice Guide: Auditing Third-party Risk Management, 2018
GTAG: Information Technology Risk and Controls, 2nd Edition, 2010

Appendix B. Glossary

Terms identified with an asterisk (*) are taken from the Glossary of The IIA's International Professional Practices Framework®, 2017 edition.

board* – The highest-level governing body (e.g., a board of directors, a supervisory board, or a board of governors or trustees) charged with the responsibility to direct and/or oversee the organization's activities and hold senior management accountable. Although governance arrangements vary among jurisdictions and sectors, typically the board includes members who are not part of management. If a board does not exist, the word "board" in the Standards refers to a group or person charged with governance of the organization. Furthermore, "board" in the Standards may refer to a committee or another body to which the governing body has delegated certain functions (e.g., an audit committee).

chief audit executive* – Describes the role of a person in a senior position responsible for effectively managing the internal audit activity in accordance with the internal audit charter and the mandatory elements of the International Professional Practices Framework. The chief audit executive or others reporting to the chief audit executive will have appropriate professional certifications and qualifications. The specific job title and/or responsibilities of the chief audit executive may vary across organizations.

compliance* – Adherence to policies, plans, procedures, laws, regulations, contracts, or other requirements.

control* – Any action taken by management, the board, and other parties to manage risk and increase the likelihood that established objectives and goals will be achieved. Management plans, organizes, and directs the performance of sufficient action to provide reasonable assurance that objectives and goals will be achieved.

control environment* – The attitude and actions of the board and management regarding the importance of control within the organization. The control environment provides the discipline and structure for the achievement of the primary objectives of the system of internal control. The control environment includes the following elements: integrity and ethical values; management's philosophy and operating style; organizational structure; assignment of authority and responsibility; human resource policies and practices; and competence of personnel.

control processes* – The policies, procedures (both manual and automated), and activities that are part of a control framework, designed and operated to ensure that risks are contained within the level that an organization is willing to accept.

engagement* – A specific internal audit assignment, task, or review activity, such as an internal audit, control self-assessment review, fraud examination, or consultancy. An engagement may include multiple tasks or activities designed to accomplish a specific set of related objectives.

engagement objectives* – Broad statements developed by internal auditors that define intended engagement accomplishments.

fraud* – Any illegal act characterized by deceit, concealment, or violation of trust. These acts are not dependent upon the threat of violence or physical force. Frauds are perpetrated by parties and organizations to obtain money, property, or services; to avoid payment or loss of services; or to secure personal or business advantage.

governance* – The combination of processes and structures implemented by the board to inform, direct, management, and monitor the activities of the organization toward the achievement of its objectives.

internal audit activity* – A department, division, team of consultants, or other practitioner(s) that provides independent, objective assurance and consulting services designed to add value or improve an organization's operations. The internal audit activity helps an organization accomplish its objectives by bringing a systematic, disciplined approach to evaluate and improve the effectiveness of governance, risk management, and control processes.

patch – Changes to a computer program designed to address a security vulnerability, an operational deficiency, or add new or upgraded features between software releases.

production environment – The setting in which software and other products become operational for their intended uses by end users.

risk* – The possibility of an event occurring that will have an impact on the achievement of objectives. Risk is measured in terms of impact and likelihood.

risk appetite* – The level of risk that an organization is willing to accept.

risk management* – A process to identify, assess, manage, and control potential events or situations to provide reasonable assurance regarding the achievement of the organization's objectives.

risk profile – A composite view of the risk assumed at a particular level of the entity or aspect of the business that positions management to consider the types, severity, and interdependencies of risks and how they may affect performance relative to the strategy and business objectives.[5]

rollback/backout plan – Plan to or process of restoring an area targeted for a potential change to its original or previous state in the event implementation or planned implementation of the potential change is found to be incorrect, unauthorized, or otherwise undesirable.

scope – The focus and boundaries of the engagement established by internal auditors that specify the activities, processes, systems, time period, and other elements that are included.

vulnerability – A condition that may expose an organization to unintended risks and consequences.

[5] Committee of Sponsoring Organizations of the Treadway Commission, Enterprise Risk Management – Integrating with Strategy and Performance https://www.coso.org/Pages/erm.aspx

Appendix C. Detailed Change Management Process

A change management process often includes the following basic steps. This list is neither complete nor exhaustive and is intended as a guide rather than a checklist. Each organization's needs will vary, and this simple tool should be customized to fit the organization.

Table C.1: Sample Change Management Process

Steps	Status
1. Identify the need for the change.	▪
2. Prepare for the change. • Document the change request in detail. • Document the change test plan. • Document a change rollback plan in the event of change failure. • Write a step-by-step procedure that incorporates the change, test plan, and rollback plan. • Submit the change procedure in the form of a change request.	▪
3. Obtain business justification. • 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.	▪
4. Obtain approval. • Gain approval from requestor.	▪
5. Authorize (via CAB). • Authorize, reject, or request additional information about the change request. • Prioritize the change request with respect to other pending changes.	▪
6. Schedule and coordinate the change. • Schedule and assign a change implementer. • Schedule and assign a change tester.	▪
7. Test in appropriate environment(s). • Test the change in a preproduction environment.	▪

8. Implement change. • Communicate the change to stakeholders who may be affected. • Approve the change for implementation. • Implement the change as requested (for software, this may require a release ticket).	▪
9. Verify/validate change. • 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 lessons were learned that may be used to improve the process? **9A. Back out of the change (if unsuccessful).** • Execute back-out procedures.	▪
10. Close request. • Conduct lessons learned. • Publish the change schedule. • Make agreed-to changes to the change management process.	▪

Appendix D. Sample Questions to Assess Effective Change Management

An organization's management should seek to understand whether change management is working effectively and efficiently by asking questions and scrutinizing the answers.

This list is not exhaustive; it is intended as a base upon which organizations can build depending on their unique situation.

Table D.1: Sample Questions to Assess Effective Change Management

- Do we have an effective change management process? Is the answer a denial of the importance of 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 reactive "firefighting" subsides?
- Have we seen benefits from the change management process? Are there measurable benefits or is the emphasis on the costs of the change management process?
- Is the enterprise-scale patch management program properly integrated with the change management system and, more broadly, the organization?
- Is the process to apply patches and security updates organized, controlled, and completed in a predictable manner?
- Has a sitewide outage occurred because of a change? Is there an understanding of how it 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 and incident reporting 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 unreliable?
- 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? Does it even have a clear focus?
- 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?
- What is the functionality and readiness of disaster recovery plan if there is an issue or a problem due to the application of a patch or an update?

Appendix E. Characteristics of Effective and Ineffective Change Management Processes

While assessing an IT change management process, internal audit should understand management's views and approach to the topic. An example of an organization whose senior management has collaborated with its IT department and has a mature and effective change management process may exhibit several of these characteristics:

Table E.1: Characteristics of an Effective Change Management Process
• Has a zero tolerance policy for unauthorized changes.
• Understands of the benefits of a robust change management process and has the ability to describe those benefits.
• Values the time and effort it takes to build an effective process.
• Is proactive and quick to identify and correct failures.
• Strives for specific and measurable goals, such as reliability, availability, and reduction of costs.
• Uses metrics to identify key indicators for successes and creating repeatable processes from those successes.
• Supports implementing root cause analysis and remedial action for identified failures.
• Has good relationships with vendors.
• Is knowledgeable about the timing of scheduled changes and patches.
• Understands how to mitigate security risks without the dangers associated with changes.

Conversely, it is also important to recognize attributes and attitudes of management with generally ineffective change management systems. These organizations may have or exhibit the following characteristics:

Table E.2: Characteristics of an Ineffective Change Management Process
• Lacks goals or metrics, failing to recognize their value.
• Justifies circumventing existing policies or controls.
• Claims implementing a sound process is too time consuming or not worth the effort.
• Spends too much time "putting out fires."
• Blames failures on a lack of budget.
• Appears resigned to accept that outages due to change are inevitable.
• Has inconsistent vendor relationships and/or blames issues on vendors.
• Does not use metrics.
• Exhibits short-sighted thinking, showing more interest in the outcome than the process.

- Does not take existing change management into consideration while implementing emerging technology with automated approval and promotion features.
- Fails to consider change management processes in the vendor selection and management processes.

Performing this indirect assessment can provide internal audit with insights to aid in the larger evaluation of the change management process as a whole.

In addition, Table E.3 compares traits of an organization with an effective versus an ineffective IT change management program in place. This list is not exhaustive but is intended to help organizations understand the positive outcomes of effective processes.

Table E.3: Change Management Processes – Effective and Ineffective Characteristics

Market Level
Effective • Company is positioned to act on new business opportunities that require additional or upgraded IT capability. • Opportunities are sufficiently planned and managed in a predictable manner. • IT-supported products and services are released to the market as planned and expected.
Ineffective • Lost opportunities. The organization is unable to consistently deploy planned new products and services. This may occur because unmanaged/mismanaged changes required the diversion of resources to unplanned work. • Development projects are late and over budget, resulting in late or costly products and services when compared to competitors.
Client Level
Effective • Adequate resources to support the client. • Products and services perform as advertised and demonstrate a consistent, reliable level of product and service quality. • Customer issues and complaints are resolved in a timely manner. • Decreasing demand for customer support center/help desk resources. • Appropriate stakeholders are involved in assessing risks associated with proposed IT changes and prioritizing their implementation. • Participants in the IT 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 IT change management, ensuring compliance with new regulations requires less effort.
Ineffective • Inadequate resources. • Products and services do not perform as advertised or as intended or operate with flaws, leading to unreliable product and/or low service quality. If customers can switch easily to another provider, they will.

Table E.3 (continued)

Enterprise Level

Effective

- 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.
- 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.
- Authorized projects are mapped to work orders and vice versa.
- More time and resources are devoted to strategic IT issues because the organization has tactical, day-to-day operational concerns under control.
- Organization demonstrates rigorous process discipline and adherence/enforcement, centralized decision-making authority, and cross-departmental communication and collaboration.
- Compliance and security investments are sustained because production configurations are maintained, thus lowering the costs of security and chances of noncompliance.
- Increasingly, more time and resources are devoted to strategic IT issues because the organization has tactical, day-to-day operational concerns under control.
- IT governance reflects control through effective change management.

Ineffective

- Unauthorized, untracked changes create potential exposure for fraud or other malicious actions.
- Business requirements can be misinterpreted with respect to required IT changes and are implemented poorly or inadequately.
- There is little to no ability to forecast the impact of a change on existing business processes.
- A lack of change prioritization, resulting in either working on the wrong things or working on something of less importance. Work may be performed out of the intended or appropriate sequence, resulting in rework and duplication of effort.
- Unauthorized, failed, or emergency patch applications occur.
- Disruptions, which not only cost time and money, but also may expose an organization to potential security risks and undesired outcomes.
- Patching systems causes disruptions due to failed changes that result in outages, service impairment, rework, or unplanned work. This may exacerbate poor or adversarial working relationships 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.
- Unmanaged changes regularly lead to the diversion of resources to rework.
- Employee turnover is high among technical staff and evidence of “burnout” exists among key staff.

Table E.3 (continued)

Infrastructure Level

Effective

- 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 changes 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 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.
- Variances in production configurations are detected early.
- 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).
- IT demonstrates efficient cost structures.
- IT quickly identifies and resolves operational problems, including security incidents.
- IT quickly returns to a known, reliable, trusted operational state when problems arise with a new change or configuration.
- Patches are implemented in a planned, predictable manner and are subject to the same analysis and process as 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.

Ineffective

- Ad hoc, chaotic, urgent behavior requires regular intervention of technical experts.
- A high percentage of time is spent in "firefighting" mode on reactive tasks.
- Inability to track changes, report on change status and costs, and there are unauthorized changes.
- Resources are spent on unplanned work at the expense of planned work.
- Numerous undocumented changes.
- Ineffective IT interfaces with peers (e.g., R&D, application developers, auditing, security, and operations) create barriers and introduce unnecessary delays.

Appendix F. Sample Change Management Audit Program

Table F.1: Sample Change Management Audit Program

Change Management Process

Control Objective: To communicate process objectives, requirements, and roles and responsibilities.

Risk: Errors are made due to lack of understanding of the process.

Control: The change management process is defined and communicated to those involved in the process, including employees and service providers.

Work Steps:

- 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

Control Objective: To delegate responsibilities such that unintentional errors or intentional, inappropriate actions will be detected.

Risk: Unexpected to adverse results.

Control: At a minimum, separate people/groups perform the responsibilities for change advisory/approval and implementation. Ideally, a separate person or group performs design change and testing of the changes. When this is not feasible or ideal, appropriate detective or monitoring controls are in place.

Work Steps:

- 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.
- Validate appropriate detective or monitoring controls are in place to mitigate or enhance segregation of duties controls.

Table F.1 (continued)

Change Management Procedures

Control Objectives:

- To ensure a change meets business needs.
- To ensure a change will not negatively impact availability, integrity, and confidentiality of systems and data.

Risk: Unexpected or adverse results.

Controls:

- A standard and centralized process exists for processing all changes.
- 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 rollback/backout plan.

Work Steps: Select a sample of changes and validate that the controls were performed from initiation through implementation of each.

Emergency Change 1

Control Objective: To ensure business needs are met.

Risk: Inability to respond effectively to emergency change needs.

Control: Procedures exist to identify, assess, and approve genuine emergency changes.

Work Steps: Select a sample of emergency changes and validate that they meet the definition/criteria of a genuine emergency change and that proper controls were performed from initiation through implementation for each.

Emergency Change 2

Control Objective: To ensure a change will not negatively impact availability, integrity, and confidentiality of systems and data.

Risk: Unexpected or adverse results.

Control: A post-implementation review is conducted to validate that emergency procedures were properly followed and to determine the impact of the change.

Work Steps: Select a sample of emergency changes and validate that they meet the definition/criteria of a genuine emergency change and that proper controls were performed from initiation through implementation for each.

Table F.1 (continued)

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

Appendix G. Sample Change Management Metrics

Table G.1: Sample Change Management Metrics
Changes Authorized and Implemented
Metric and Indicator: Number of changes authorized and implemented per standard change window.
Guidelines: In general, more changes equate more change productivity as long as the change success rate remains high. Trending of this number over time can help establish a baseline of the anticipated number of changes at a given time of year based on the business operating cycle.
Changes Made in Production
Metric and Indicator: Number of changes actually made in production per standard change window. This could be measured through a detective control such as monitoring software or through monitoring the number of deployments made by application developers.
Guidelines: Any number that deviates from the number of changes authorized per window should be thoroughly investigated (because a single rogue change may have severe system and business impacts).
Changes Implemented
Metric and Indicator: Change success rate, defined as the number of changes implemented (i.e., changes which did not cause an outage or result in any service impairments) compared to the total number of changes approved during the change window.
Guidelines: Higher is better. High-performing organizations have successful change rates at or near 100% with deviations regularly investigated. Additionally, high-performing organizations that may experience a failed change generally do not experience service impacts because a well-understood backup/rollback plan is in place. Organizations that do not sufficiently test, approve, and manage changes may experience lower success rates.
Changes Lacking Sufficient Testing
Metric and Indicator: Percentage of normal changes approved for production lacking sufficient testing evidence or results.
Guidelines: Lower is better. Normal (nonemergency changes) changes should all be sufficiently tested prior to approval with testing results indicated in the change request.
Normal Changes vs. Other Types
Metric and Indicator: Percentage of normal changes compared to other change types (e.g., emergency, blanket changes). Blanket changes are typically recurring changes that are low risk and well understood. Due to the low level of risk posed by these types of changes, they may not require the same level of testing or approval prior to implementation. An example of a blanket change could be a normal application update for a non-enterprise application.
Guidelines: Higher is typically better as the majority of changes should be normal and therefore subject to the full change management process. However, a moderate percentage of blanket changes is acceptable since the risk posed by these types of changes are nominal.
Unplanned Work
Metric and Indicator: Percentage of time spent on unplanned work. Unplanned work is caused by addressing issues resulting from unsuccessful changes, or break/fix items.
Guidelines: Lower is better (e.g., 5% or less).

Appendix H. References and Additional Reading

References

Buckley, Shannon. “IT Change Management,” *Internal Auditor*, September 1, 2011, https://iaonline.theiia.org/it-change-management.

CISA Cyber+Infrastructure, Department of Homeland Security. Accessed January 20, 2020. https://www.us-cert.gov/.

Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management – Integrating with Strategy and Performance.* https://www.coso.org-/Pages/erm.aspx

National Vulnerability Database, NIST. Accessed January 20, 2020. https://nvd.nist.gov/.

U.S. House of Representatives Committee on Oversight and Government Reform. “The Equifax Data Breach.” Majority Staff Report, 115th Congress. December 2018. https://republicans-oversight.house.gov/wp-content/uploads/2018/12/Equifax-Report.pdf.

Additional Reading

Bonney, Bill, Gary Hayslip, and Matt Stamper. *CISO Desk Reference: A Practical Guide for CISOs.* San Diego: CISO DRG, 2019. https://bookstore.theiia.org/ciso-desk-reference-guide-a-practical-guide-for-cisos.

Buckley, Shannon. “Auditing the Incident and Problem Management Process.” *Internal Auditor*, January 1, 2012. https://iaonline.theiia.org/auditing-the-incident-and-problem-management-process.

Gibbs, Nelson, Divakar Jain, Amitesh Joshi, Surekha Muddamsetti, and Sarabjot Singh. *A New Auditor's Guide to Planning, Performing, and Presenting IT Audits*. Altamonte Springs, FL: The IIA Research Foundation, 2010. https://bookstore.theiia.org/a-new-auditors-guide-to-planning-performing-and-presenting-it-audits.

Mahfuz, Abu Sayed. *Software Quality Assurance: Integrating Texting, Security, and Audit.* UK: CRC Press: An Auerbach Book, 2016. https://bookstore.theiia.org/software-quality-assurance-integrating-testing-security-and-audit.

Whittaker, Zack. “Equifax breach was ‘entirely preventable’ had it used basic security measures, says House report,” TechCrunch.com, December 18, 2018, https://techcrunch.com/2018/12/10/equifax-breach-preventable-house-oversight-report/.

Acknowledgements

Guidance Development Team

Susan Haseley, CIA, CISA, United States (Chair)

Scott Moore, CIA, CRISC, CISA, GSLC, United States (Team Lead)

Lee Keng “Joyce” Chua, CIA, Singapore

Manoj Satnaliwala, CIA, United States

Content Contributors

Brad Ames, United States

Jim Enstrom, United States

Mueni Kioko, The Bahamas

Mike Lynn, CIA, CRMA, United States

Sajay Rai, CISM, CISSP, CISM, United States

Terence Washington, CIA, CRMA, United States

Shawna Flanders, Director of IT Curriculum, IIA Staff Contributor

IIA Global Standards and Guidance

P. Michael Padilla, CIA, Director (Project Lead)

Jim Pelletier, Vice President

Cassian Jae, Managing Director

Anne Mercer, CIA, CFSA, Director

Chris Polke, CGAP, Director

Jeanette York, CCSA, Director

Shelli Browning, Technical Editor

Lauressa Nelson, Technical Editor

Geoffrey Nordhoff, Content Developer, Technical Writer

Vanessa Van Natta, Standards and Guidance Specialist

The IIA thanks the following oversight bodies for their support: Information Technology Guidance Committee, Professional Guidance Advisory Council, International Internal Audit Standards Board, Professional Responsibility and Ethics Committee, and the International Professional Practices Framework Oversight Council.

About The IIA

The Institute of Internal Auditors (IIA) is the internal audit profession's most widely recognized advocate, educator, and provider of standards, guidance, and certifications. Established in 1941, The IIA today serves more than 200,000 members from more than 170 countries and territories. The association's global headquarters is in Lake Mary, Fla., USA. For more information, visit www.globaliia.org.

Disclaimer

Copyright

February 2020

Note: The cover, logo, and certain references were updated November 2021. There were no changes to the original content. Questions may be directed to guidance@theiia.org.

The Institute of Internal Auditors

Global Headquarters
The Institute of Internal Auditors
1035 Greenwood Blvd., Suite 401
Lake Mary, FL 32746, USA
Phone: +1-407-937-1111
Fax: +1-407-937-1101