IT AUDIT CHECKLIST SERIES

ComplianceINSIGHT

Change Management

Practical guidance for managers on how to prepare for successful audits

www.ITCinstitute.com

IT Compliance Institute™

Research Sponsors

Solidcore

Tripwire

ComplianceINSIGHT

IT AUDIT CHECKLIST SERIES

Change Management

About the IT Compliance Institute

The IT Compliance Institute (ITCi) strives to be a global authority on the role of technology in business governance and regulatory compliance. Through comprehensive education, research, and analysis related to emerging government statutes and affected business and technology practices, we help organizations overcome the challenges posed by today's regulatory environment and find new ways to turn compliance efforts into capital opportunities.

ITCi's primary goal is to be a useful and trusted resource for Information Technology professionals seeking to help businesses meet privacy, security, financial accountability, and other regulatory requirements. Targeted at CIOs, CTOs, compliance managers, and information technology professionals, ITCi focuses on regional- and vertical-specific information that promotes awareness and propagates best practices within the IT community.

For more information, please visit: www.itcinstitute.com

Comments and suggestions to improve the IT Audit Checklists are welcome. Please send your recommendations to editor@itcinsititute.com.

Table of Contents

Executive Overview

What Is the IT Audit Checklist Series?

The ITCI IT Audit Checklists are a series of topical white papers that provide practical guidance for IT, compliance, and business managers on preparing for successful internal audits of various aspects of their operations. In addition to helping managers understand what auditors look for and why, the IT Audit Checklists can also help managers proactively complete self assessments of their operations, thereby identifying opportunities for system and process improvements that can be performed in advance of actual audit.

What Is This Paper About?

This paper, "IT Audit Checklist: Change Management," supports an internal audit of the organization's change management policies in order to verify compliance and look for opportunities to improve efficiency, effectiveness, and economy. The paper includes advice on assessing the existence and effectiveness of change management in project oversight, development, procurement, IT service testing, and IT operations; guidance for management and auditors on supporting change management; and information on ensuring continual improvement of change management efforts. The paper is intended to help IT, compliance, audit, and business managers prepare for an audit of high-level processes and resources and provide concrete tools managers can use to ensure that the audit experience and results are as beneficial as possible to both IT leaders and the company as a whole.

Paper Contents

- Regulations such as Sarbanes-Oxley and Basel II have exposed the reality that IT processes do not merely underlie business processes: in many cases, they are indistinguishable. As companies have grown more dependent on interdependent IT systems, the risks associated with untested changes in development and production environments have increased proportionately.
- Change management limits the risks associated with the introduction of new elements and other modifications in IT environments, focusing on prevention of unapproved ad hoc changes and rapid recovery from change-related problems.
- Change management control objectives, policies, and procedures should encompass both human errors and malicious endeavors. Effective change management controls risks without compromising business agility.
- This document provides a "base" IT audit checklist you can use and modify to fit your specific situation. Controls cited in this paper are derived from Control Objectives for Information Technology (CobiT) from the Information Systems Audit and Control Association (ISACA); ITIL from the UK Office of Government Commerce (OGC); Special Publication 800-53, "Recommended Security Controls for Federal Information Systems" from the National Institute of Standards and Technology (NIST); and the authors' own experience.
- In general, control objectives are categorized as management, operational, or technical, following the grouping mechanism in NIST 800-53. However, cited change management control objectives go beyond NIST's recommended controls for information security to address change considerations for

project management, development, procurement, service testing, IT operations, and other key business processes.

- Change management audits are opportunities for companies to improve, based on auditor analysis and advice. To preserve the integrity and authority of audits, auditors must maintain a delicate balance between offering advice and making decisions.
- Managers, not auditors, are ultimately responsible for defining and implementing solutions to issues found in the audit. Thus, it is in everyone's best interest to have a cooperative, collaborative audit process that respects the independence and discretion of all participants. Auditors should listen to management, and management should encourage staff to be open and honest with auditors.

Introduction to Change Management

IT organizations are besieged by seemingly contradictory mandates. They must contain costs in the face of swelling demands and system volume. At the same time, they are expected to provide unlimited services within the limitations of risk thresholds, and they must meet increasing functional demands in increasingly complex environments under stringent management and deadlines. And in the process they must hit an ever-increasing number of control "checkpoints" between conceptualization and implementation.

Central to meeting all of these challenges is the factor of change: how organizations, technologies, user expectations, oversight, and risk management are evolving and impacting businesses. As companies become more dependent on interdependent IT systems, the risk associated with untested changes in development environments increases almost exponentially. Meanwhile requirements for privacy and integrity of sensitive data in production systems indicate the need for companies to monitor changes to system access controls. And globalization of the IT labor market—and management challenges associated with a distributed workforce—is sparking awareness of the need for special oversight of outsourcers and the changes they make.

In fact, the list of potential changes that can impact a company is almost as vast and multiform as the universe of IT systems and corporate organizations. As a practice, change management attempts to tame this multitude by systematically controlling sources and types of changes that have significant or material risk potential. This acknowledged relationship of change to risk also means that internal auditors are increasing the frequency and "depth" of their assessments of change management policies and processes.

What Is Change Management?

The goal of change management is to limit risks associated with the introduction of new elements and other modifications into an IT environment; particularly, in development, project management, procurement, outsourcing, service testing, and operational areas. Effective change management achieves these control goals without compromising business agility.

To ensure that IT risks are understood and properly addressed, it can be useful for IT management to adopt a service management mindset. Traditionally, IT has seen itself primarily in terms of providing infrastructure and applications to business users. This scope might have been sufficient, as long as IT operated primarily as a tactical and technical department, but the rapid evolution of IT into a strategic factor and even business competency of its own accord require a maturation of IT management concepts.

Recent regulations, such as Sarbanes-Oxley and Basel II, have exposed the reality that IT processes do not merely underlie business processes. In many cases, the two are indistinguishable. Accordingly, IT management (and controls) must proactively address not only software and software development, but hardware, staff, documentation, facilities, vendors, processes, and other integral components required to meet the needs of the business. The use of the word "service" in the remainder of this paper reflects this inclusive concept.

ITIL terms such service elements "configuration items" and requires IT to define their relationship to one another, in order to deliver the service the business needs. The concept of relationships and all of the risks it might imply—misalignment, disruption, repurposing, even destruction—is critical to the concept of change management. In the traditional IT view, ad hoc application changes, for example, had very localized effects and little risk. But in reality, even small changes in today's complex, highly integrated IT environments can have massive unintended downstream effects.

Thus, prevention of unapproved ad hoc changes is at the heart of change management. Essentially, all changes must be separately reviewed and approved prior to implementation. Management defines an appropriate change model, or workflow, for change requests based on their potential business impact and urgency. An assigned review authority either approves the change and schedules it for implementation or rejects the change and returns it to the requestor with an explanation. This basic workflow can be expanded or contracted, in relation to the nature of the change. After all, the purpose of change management policies and procedures is not to impede development, but rather to provide controls that balance the need for the organization to change against change-related risks.

The other fundamental goal of change management is rapid recovery from change-related problems, when they arise. Versioning and back-out plans are critical controls that help organizations recover from system failures related to patches, upgrades, updates, and other revisions that, for one reason or another, take a production system down when they go live. Versioning is essentially a series of backups (and metadata) of known working system states prior to any significant change. Back-out plans are procedural documents that detail how staff should respond to a change-related failure, back out of problematic processes, restore a working system or database, and change procedures to prevent future such events. Versioning and recovery planning are critical preventative controls. Unfortunately, many companies don't think about them until they are in the midst of a failure and the damage is already excessive.

What Are the Benefits of Change Management?

Because change management provides a formal means to control changes, it is ideal for limiting a variety of behaviors stemming from malicious acts and human error. In fact, it is the latter that presents most risk to organizations, as employee mistakes are the most common source

of IT and business errors. Thus, the scope of change management control objectives, policies, and procedures should encompass both mistakes and malice.

In general, change management can help an organization reduce risks to a level acceptable to management. Appropriate change management controls benefit not only regulatory compliance, but information security, operations, and risk management functions. Moreover, since the goal of change management is largely to ensure that changes are appropriate and don't product negative consequences, good change management controls can actually support both IT and business agility.

Specific benefits of sound change management include:

Project Management

- Less opportunity for scope creep and requirement changes
- Stronger adherence to budgets, milestones, and deadlines
- Improved product and project transparency during development process
- Predictable project outcomes; better alignment with management expectations
- Ability to more tightly track developer time expenditures
- Opportunity to gain progressive buy-in from business stakeholders on midproject functional revisions
- Higher confidence in IT staff by business sponsors and stakeholders

Development

- Better alignment of product functionality with requirements and expectations
- Fewer certification issues stemming from lack of change management controls
- Lower scrap and rework costs associated with inappropriate and nonfunctional development
- Demonstrable integrity of proprietary code; preservation of intellectual property value
- Lower risk of negative impact on production systems from unapproved changes
- Tighter management of staff resources, time spent on projects, and adherence to deadlines
- Necessary creation of stable application testing environment, wherein functional variables can be carefully controlled
- Less cost and delay associated with reconciling applications across inconsistent of development, test, and production environments

Procurement

- Congruity between contracted work and actual scope of work
- Better oversight of change orders and change-related project costs
- Better alignment of planned and actual services—and planned and actual risk levels—associated with externally developed applications

IT Operations

- Stronger technical security controls for information confidentiality, integrity and availability
- Less opportunity for human error; smaller "blast radius" for errors that do occur
- Less unplanned IT work, enabling focus on core activities and planned initiatives, such as preventive maintenance and projects
- Faster recovery from unplanned failures and downtime as a result of system upgrades and changes
- Faster identification of unauthorized changes or system access based on comparison of existing production environment to "last known good state" system image

- Faster identification of control deficiencies allowing unauthorized changes, based on change monitoring; faster response to and remediation of security events
- Faster, more effective staff response to system crashes due to software changes or other factors, such as spontaneous hardware failure
- Higher customer satisfaction and an improved perception of IT by management, based on improvements to information confidentiality, integrity, and availability, as well as worker productivity
- Fewer business losses due to change-based failures of production systems

The Auditor's Perspective on Change Management

Why Audit?

Change management audits are opportunities for companies to improve, based on auditor analysis and advice. To preserve the integrity and authority of audits, auditors maintain a delicate balance between offering advice and making decisions.

For each organization, the scope of auditor responsibility should be documented in the company's internal audit charter and be approved by the audit committee. Because each organization has different goals and objectives—and certainly different issues and challenges—there is no one-size-fits-all audit process, nor one audit approach, that fits all situations.

Audits should ensure that management and staff understand and adhere to change management policies and procedures. Because change management is itself a risk management control, failure to follow mandated processes means that risks to the organization are not being properly mitigated.

The size and complexity of various organizations' audit efforts differ due to variations in operating environments, risk priorities and thresholds, and business and audit objectives. In addition, the scope of audits can vary from project to project, depending upon an auditor's focus (for example, on various business processes, management controls, and technical controls). Ensuring appropriate audit focus is another reason management should communicate with auditors, and vice versa, early and often for every audit project.

Internal auditors should perform organizational risk assessments and evaluate the audit universe and supporting audit plans at least annually and sometimes more frequently. At the micro level, an audit risk assessment of the various entities being audited is completed to support the audit project (sometimes also referred to as

the audit "terms of reference"). Planning for each audit requires serious consideration of the organization's many risks and opportunities. Finally, in many companies, continuous auditing (ongoing audit evaluations) is being implemented for key systems and/or key transactions.

Who Is Responsible for Change Management?

Management (of IT, staff, and business lines) and internal auditors all have significant roles in change management assurance and the auditing of change management controls. The big question for many companies is how these stakeholders should work together to ensure that everything that should be done to protect sensitive systems is being done—and that the company's information assets are protected appropriately.

1. **Executive management** must provide leadership and set the correct tone from the top to ensure that change management efforts are supported and understood across the organization—and demonstrating by example compliance with change management policies.

   Executive management must also dedicate sufficient resources to allow controls to be effective. The workflows, approvals, and testing requirements required by change management policies commonly add steps to companies' standard development processes. Executive management should support and reinforce the message that these steps are necessary and encourage IT managers, project managers, and business stakeholders to schedule necessary time and staff for proper control adherence.

   Finally, by ensuring that the change management program and its management are subject to audit and reviewed by qualified professionals, corporate leaders advance the goal of corporate oversight and promote its continuous improvement and success.

2. **IT management** must have a voice in the design and implementation of change management programs, since they are held accountable for protecting and enhancing the value of the organization's technologies, applications, and systems. Managers must also review and monitor change management controls to ensure they are appropriate, despite ever-changing risks and business requirements. This is, in fact, a form of auditing.

3. In addition to these general roles, ITIL identifies three roles specific to change management that should be identified in relation to any planned changes and projects:

   The **change owner** is the managerial sponsor of the change management process. This person is responsible for ensuring the new mandates are followed. In order to facilitate any cultural change necessary to support technology and process changes, the change owner must have enough political power to get stakeholder buy-in and, if possible, enforce compliance.

   The **change manager** is the person accountable for the day-to-day process. This person has ultimate authority to approve and reject change requests, and is responsible for reviewing, filtering, and identifying which change management model a given request should follow. The change manager follows the change process and manages risks associated with changes.

   The **change controller** is an optional role for organizations that require a coordinator between the change manager and various people and functions responsible for implementing the change. Tasked with administrative work and other formally delegated tasks, the change controller position is intended to give the change manager sufficient support to effectively oversee the change management process.

   These roles aren't necessarily congruent with organizational titles, although they can be dedicated roles. Thus, a data center manager might be both the change owner and change manager for a particular request. Alternatively, the change owner could be the

businesses user who requested the change or even the vice president of operations. And Change Manager might be an assigned IT title. Who has the roles is less important than that change management policies and procedures identify the roles and responsibilities, and that job descriptions reflect these requirements.

4. The **internal audit** function provides strategic, operational, and tactical value to an organization. In relation to change management, for example, internal audit:

    - Informs the board and management as to whether business and IT units understand the importance of change management and are adhering to policies, whether key information assets and systems are sufficiently protected, whether programs are in place for continually updating and strengthening safeguards against unauthorized changes and undue risk stemming from authorized changes, and whether existing policies are reasonable and enforced. In brief, internal audits assess the state of the change control environment and recommend improvements.

    - Independently validates that the organization's change management efforts are proactive and effective against current and emerging threats. To provide this level of assurance, internal auditors may compare current organizational practices with industry practices and regulatory guidelines.

Of course, auditing provides only a reasonable level of assurance. Auditors cannot provide an insurance policy against any fault or deficiency, particularly in regard to activities that cannot be totally controlled, such as management-approved exceptions to mandated policies.

To fulfill the audit's potential, however, internal auditors need to:

1. Know what they are doing (have the skills to perform appropriate change management audits)

2. Have a strong understanding of the technical and the business environment and factors that might influence the effectiveness of change controls

3. Know what to ask for in assessing change management programs

4. Complete regular and ongoing training to keep on top of new guidance and standards of practice

In addition, the auditing function should complement, but never replace or overpower, management's responsibility to ensure that change management controls are existent and effective.

Management's Role in the Audit Process

An internal audit engagement typically has three phases: planning, testing, and reporting. Management has an important role in each phase:

- ☐ **During planning**, management should first focus on the audit plan (the auditor's "road map") and ensure that managers understand and are generally agree with the audit purpose, focus, and approach. An open, positive discussion with the audit team regarding these defining factors helps management and the audit team communicate their expectations up front. Audit planning should focus on critical or sensitive risks, but all risks should be considered. To this end, active involvement by management in audit planning is vital to the overall success of an internal audit.

  Management should also discuss the evaluation criteria auditors will use in assessing change management controls. Finally, managers and auditors should broadly discuss how auditors plan to test existing controls, although auditors ultimately have the authority and discretion to select tests they deem appropriate.

- ☐ **During testing**, management facilitates the auditors' access to appropriate people and systems. Management confirms the audit results, not re-performing the actual tests, but verifying processes and data in order to gain confidence in the audit findings. The audit team leader and senior executives of the areas being audited should meet regularly throughout the audit process—usually weekly and at least once a month—to discuss audit progress, identified issues, and potential actions.

  An open, transparent dialogue between senior members of both management and the audit team does much to avert misunderstandings or resolve disputed findings before the audit team issues its draft report. The audit team should communicate critical findings to management as early as possible, even outside of the established meeting schedule. These findings may also be reviewed during regular meetings, but prompt notice is necessary and usually appreciated.

- ☐ **During reporting**, management receives and reviews the findings of auditors, plans and develops corrective actions, and implements change.

Managers and auditors should work together throughout the audit process to ensure that auditors pursue appropriate goals and have proper insight into IT and business processes. Good communication throughout the audit process helps ensure that audit findings are relevant and can be used to benefit the company.

What Auditors Want to See

Audits exist to assess how well a business unit or program meets the performance goals of the organization, as dictated by the CEO, CFO, board, and investors. Accordingly, the managerial goal in auditing is not simply to make auditors happy, but to demonstrate how well operations, controls, and results meet the needs of the business. During audit planning, managers help auditors to design an audit process that truly reflects business strategies and goals. Thus, the managerial response to auditors throughout the audit process—planning, testing, and reporting—is for the benefit of the business, not its auditors.

Auditors exist to provide the board and senior management with an objective, independent assessment of a business unit or program (such as change management), including what they see as key opportunities for improvement. To prepare their opinions and conclusions, auditors need to review and assess evidence of the risk management program and its performance. If auditors are able to demonstrate performance and show that accountability has been established and is working, they should produce a positive audit report.

Accordingly, auditors and managers should work to help each other reach common goals—auditors striving to earnestly, honestly, and completely assess program effectiveness, and management working to help auditors make valid assessments. In that vein, there are some typical program characteristics and managerial processes that auditors do and don't like to see. As in all aspects of audit and risk management programs, auditor likes and dislikes vary by company; however, the following list itemizes typical indicators of good and bad audits.

Auditors Like ...

- ☐ Good management practices: planning, direction, monitoring, reporting, etc.
- ☐ Proactive management including frequent, if not continuous, operational monitoring
- ☐ Supervisory review of key performance reports and operating results
- ☐ Organized, clear, and up-to-date documentation
- ☐ Well documented policies and procedures
- ☐ Managerial actions based on facts, not habits
- ☐ A documented chain of command, roles, accountability, and responsibilities
- ☐ Consistent adherence to policy and procedures, from senior management through frontline staff
- ☐ Good staff management, including workforce development (bench strength and cross training), assurance that absences do not compromise controls, and policies for secure staff turnover
- ☐ A balance between short- and long-term focus, for both objectives and results
- ☐ Managerial willingness to embrace new ideas

Auditors Don't Like ...

- ☐ Managers who adopt the "letter" of change management requirements in order to satisfy audit requirements, rather than embracing the "spirit" of the controls for the full risk mitigation they can offer
- ☐ Interviewing defensive or uninformed managers and executives
- ☐ Wading through piles of disorganized analyses
- ☐ Managers who can't or won't comprehend the level of risk they are incurring
- ☐ The opposite of the "like" items listed above

How Companies Help (or Hinder) Auditors

- ☐ (Not) having requested documentation available at the prearranged time
- ☐ (Not) meeting deadlines and (not) stonewalling
- ☐ (Not) communicating at an appropriate managerial level
- ☐ (Not) ensuring key staff are available to auditors, especially at critical milestones
- ☐ (Not) informing relevant staff about the audit and its goals, affecting the time and effort auditors must spend to explain the audit to affected personnel
- ☐ (Not) having administrative support where needed
- ☐ (Not) providing accurate documentation
- ☐ (Not) having an audit charter for the internal audit function

Who Should Talk to the Auditors?

An efficient audit process depends on effective communication between auditors, managers, and workers. Management and auditors should strive to balance efficiency (having a minimal number of staff dealing directly with the auditors) with the need for "open access" to management and staff by the audit team (when needed).[1] Obviously, it is impractical and unproductive for both teams to put too many staff in front of auditors. Instead, management should:

- ☐ Provide knowledge of operations through several informed "point" people to interact with auditors. A "short list" of interviewees within the program area being audited can more quickly answer auditor queries and provide better continuity of audit support.
- ☐ Allow ready access to all management and staff, if required by the audit team to gain a clearer picture of overall operations
- ☐ Work with the audit team to draw up a staff interview schedule as part of the planning effort. Update the schedule as necessary during the audit fieldwork phase, if circumstances change.

In many situations, a single point of contact for each audited program provides the vast majority of documentation to the audit team. The role of that individual—and, indeed, for all auditor contacts—is to ensure that the audit team receives accurate and adequate information for the task. Auditors still use their professional judgment to determine if and when additional sources of information (other staff interviews) are required. The audit team also conducts a variety of audit tests, if necessary, to confirm their audit analysis.

[1] The audit team is always expected to ensure all their interactions (with all staff) are professional and result in a minimal disruption.

Change Management Audit Checklist

Your audit's goals, scope, and purpose determine the appropriate audit procedures and questions. An audit of change management controls should determine that key risks to the organization are being controlled, that key controls are operating effectively and consistently, and that the relevant functional area management and staff have the ability to recognize and respond to new threats and risks as they arise.

The following checklist generally describes change management audit steps that management might follow in preparation for and during an audit. The list does not attempt to itemize every possible change management objective, but rather to provide general guidance on defensible controls and a logical control hierarchy.

Audit Planning

- ☐ The audit team develops an initial draft of the internal audit plan
- ☐ Those change owner, change manager, and other stakeholders meet with the audit team to review audit program steps and define key players and necessary resources
- ☐ Change management staff collects program documentation in preparation for audit
- ☐ Management supports a preliminary survey of the change management program (by the internal audit team)
- ☐ The audit team drafts the internal audit program plan
- ☐ Management and board members provide feedback on the draft plan

Audit Testing

Management has a responsibility to ensure that audit testing is productive. The audit team performs tests to independently assess the performance of the change management program. Although the audit team ultimately determines the nature of these tests and the extent of testing (e.g., the sample sizes to use), management should engage auditors in discussions about their testing methods and goals.

In tone, management should try to strike a balance, neither entirely deferring to the audit team nor micromanaging the internal audit efforts. The key is to provide productive input on the evaluation methodology before audit management signs off on it.

As the testing phase winds up, the audit team prepares summaries of its key findings. Change managers (or IT management responsible for interacting with auditors on their behalf) should be prepared to provide feedback and comments on audit summaries, prior to the more final, formal audit report.

Proactive communication, candor from all parties, and thorough documentation can prevent many surprises and conflicts that might otherwise arise during the testing phase; however, managers might still disagree from time to time with audit results. Management should strive to provide solid evidence—not just argument—that supports its contrasting position. Facts are the most powerful tool for swaying an adverse opinion before the audit report is finalized.

Since the audit report often forms the basis of future change management control development and support, management should ensure that every audit point raised—and its related recommendation—is relevant and valid. Likewise, every action plan proposed by managers or auditors should be achievable, appropriate, cost effective, and able to produce lasting effect.

Audit Testing Processes

- ☐ Managers and auditors complete a "kick-off" meeting
- ☐ Managers support auditors' assessment of change management controls with interviews and documentation of:
  - ___ Scope and strategy, including how thoroughly the controls addresses potential risks and compares with industry best practices
  - ___ Structure and resources, reflecting managerial commitment to effective change management and the program's robustness relative to the potential impact of adverse events
  - ___ Management of policies and related procedural documentation
  - ___ Communication of program policies and expectations to stakeholders
  - ___ Impact of program efforts on organizational culture
  - ___ Internal enforcement processes and consistency
  - ___ Ongoing improvement efforts
- ☐ Managers support more detailed audit analysis of the change management program
- ☐ Auditors complete the evaluation of design adequacy
- ☐ Auditors complete the evaluation of control effectiveness

Audit Testing Steps

The following activities may be repeated in each of the aforementioned audit processes.

- ☐ Auditors evaluate information on change management processes and procedures
- ☐ Managers assist auditors with walkthroughs of selected processes and control documentation
- ☐ Auditors evaluate the quality of information generated by the change management program, considering the ease, reliability, and timeliness of access to such information by key decision makers; and the operational consistency with which such information is generated
- ☐ Auditors assess change management performance metrics: existence, effectiveness, monitoring, and responses to deviation
- ☐ Auditors evaluate whether risk management controls are sufficiently preventive, detective and, if applicable, corrective
- ☐ Auditors define tests to confirm the operational effectiveness of change management activities. Tests might include management and staff interviews, documentation and report review, data analysis, and result sampling for recent initiatives.
- ☐ Managers provide requested data, documentation, and observations
- ☐ Auditors identify and recommend opportunities for improvement of change management activities
- ☐ Managers and auditors complete an exit meeting to discuss audit findings, auditor recommendations, and managerial response

Controls for Change Management

The objectives cited in this section represent a "menu" of widely accepted change management controls that the reader may organize, cull, and implement in a manner that meets unique organizational requirements. Objectives are drawn from Control Objectives for Information Technology (CobiT)[2] from the Information Systems Audit and Control Association (ISACA); ITIL[3] from the UK Office of Government Commerce (OGC); Special Publication 800-53,[4] "Recommended Security Controls for Federal Information Systems" from the National Institute of Standards and Technology (NIST); and the authors' experience. In evaluating an organization's change management, auditors might review the controls listed in this section—and potentially others, depending on the audit's purpose and focus.

In general, control objectives are categorized as management, operational, or technical, following the grouping mechanism in NIST 800-53. However, cited change management control objectives go beyond NIST's recommended controls for information security[5] to address change considerations for project management, development, procurement, service testing, IT operations, and other key business processes.

The actual change management controls to be audited are determined during the audit planning phase. Controls are assessed during the audit testing phase. Management should determine which change management controls are appropriate for each organizational environment, based on the corporate risk profile, and compare the list to the controls in this section, which reflect audit best practices.

The organizational approach to change management is reflected in Figure 1, which reflects CobiT's IT control structure. Change management controls (including access controls that protect information integrity) should be considered throughout any development or implementation cycle—from planning through delivery and post-implementation evaluation.

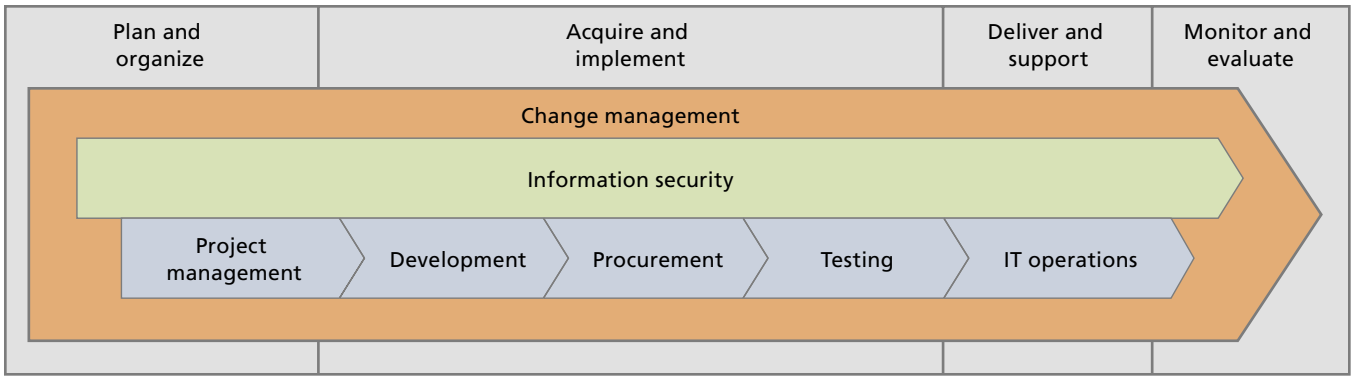

Figure 1: An operational approach to change management.

[2] Information Systems Audit and Control Association (ISACA), "Control Objectives for Information and related Technology (COBIT)": http://www.isaca.org/cobit

[3] UK Office of Government Commerce Information Technology Infrastructure Library v3. June 2007. http://www.itil.co.uk

[4] US NIST Special Publication (SP) 800-53, Recommended Security Controls for Federal Information Systems. February 2005. http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf

[5] NIST 800-53 and an additional publication, FIPS 199 ("Standards for Security Categorization of Federal Information and Information Systems" <http://csrc.nist.gov/publications/fips/fips199/FIPS-PUB-199-final.pdf>. February 2004.), provide much more extensive guidance on information security controls than is reproduced in this paper. Of particular note is the three control impact ratings or "baselines" defined in FIPS 199 and specified for individual controls in NIST 800-53. The NIST guidelines do not simply assign each control a baseline; rather, they provide guidance on how controls must be implemented to meet the criteria for increasingly stringent levels of control baselines.

Management Controls

Management controls ensure a well-run and effective change management program. In general, management controls assess whether:

- ☐ Change management policies and procedures have been established
- ☐ Performance is measured using established and documented metrics
- ☐ Budgets support actual change management requirements
- ☐ A continuous improvement program is in place and operates effectively
- ☐ A disciplinary process exists for personnel who choose not to follow change management procedures

More specifically, change management control objectives include:

Risk Assessment (RA)

Organizations must periodically assess the risk to organizational operations (including mission, functions, image, or reputation), organizational assets, and individuals, resulting from the operation of organizational information systems and the associated processing, storage, or transmission of organizational information.

	Description
☐	**Risk Assessment Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented risk assessment policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the risk assessment policy and associated risk assessment controls
☐	**System Risk Profile:** The organization categorizes the IT system, processes, and services, including 1) business purpose, 2) impact on the business in terms of dollars (or other relevant goal units), 3) business owner, 4) data owner, 5) relationships of various configuration items (for example: parent-child relationships) within systems and services, 6) security requirements, and 7) other data relevant to the business
☐	**Risk Assessment:** The organization conducts assessments of the risk and magnitude of harm that could result from the unauthorized access, use, disclosure, disruption, modification, or destruction of information and information systems that support the operations and assets of the agency
☐	**Risk Assessment Update:** The organization updates the risk assessment whenever there are significant changes to the information system, the facilities where the system resides, or other conditions that may impact the security or accreditation status of the system

Management Controls

Assessment and Managerial Certification of Change Management

Management actively oversees policies and processes related to IT product and service changes and related risks.

Description

- ☐ **Change Management Assessment Policies and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) documented change management assessment and certification policies that address purpose, scope, roles, responsibilities, and compliance; and 2) documented procedures to facilitate the implementation of the change management assessment and certification policies and associated assessment, certification controls
- ☐ **Change Management Assessment and Certification:** The organization conducts an assessment of change management controls to determine the extent to which the controls are functional and effective
- ☐ **Plan of Action and Milestones:** The organization develops and updates a plan of action and milestones that documents the organization's planned, implemented, and evaluated remedial actions to correct any deficiencies noted during the assessment of change management controls and to reduce or eliminate known vulnerabilities in the information system
- ☐ **Continuous Monitoring:** The organization monitors change management through key performance indicators (KPIs), including 1) number of changes authorized per week, 2) number of changes implemented per week, 3) number of unauthorized changes detected, 4) change success rate, 5) number of changes resulting in service affecting outages, 6) amount of downtime in hours resulting from unauthorized changes, 7) cost of downtime associated with unauthorized changes, 8) number of emergency changes, and 9) number of standard changes

Planning

In each area that requires change management, proper planning is vital to mitigate organizational risks and optimize efficiency, effectiveness, economy, and compliance. Organizations must develop, document, periodically update, and implement change management plans for organizational information systems that describe the change management controls in place or planned.

Description

- ☐ **Change Management Plan:** The organization develops, documents, and implements a change management plan that provides an overview of change management requirements for the services and a description of controls in place or planned for meeting those requirements. The plan clearly identifies scope of coverage of change management policies and procedures and identifies change management controls based on the specific characteristics and requirements of particular staff groups or environments (e.g., production environments vs. development environments, onsite vs. offsite developers, internal vs. contracted developers, etc). Designated officials within the organization review and approve the plan.
- ☐ **Change Management Plan Updates:** The organization has a defined review period, reviews the change management plan, and revises the plan to address system/organizational changes or problems identified during plan implementation or security control assessments

Management Controls

Planning *(continued)*

Description

☐ **Change Management Models:** The organization develops a variety of change models and defines clear criteria for when each model should be applied. Models indicate varied workflows and processes to accommodate variations in risk and urgency associated with different scenarios and requirements. Common change management models include:

- Standard: Simplified policies and processes associated with low-risk changes—generally comprising a single review, approval, and logging
- Significant: Policies and procedures associated with higher-risk changes, often requiring the involvement of a change advisory board (CAB) to evaluate and accept or reject the proposed change
- Emergency: Polices that support abbreviated change management processes in the case of an urgent need. Emergency procedures support rapid implementation of a change and forestall thorough testing and verification until after the crisis has passed.

All change models reduce residual risk to a level acceptable by management. Each model defines testing protocols commensurate with associated risks.

☐ **Scheduling:** In order minimize the disruptive impact of changes on the business and prevent change scheduling conflicts, the organization: 1) defines maintenance windows for IT services, 2) manages change scheduling through a "forward schedule of change," 3) documents and any planned downtime beyond that defined in the negotiated maintenance windows in a planned service availability (PSA) document, and 4) evaluates the success or failure of changes following implementation.

Changes that must be scheduled outside of planned maintenance windows follow a defined emergency change model that defines: 1) criteria for allowing exceptions, 2) individuals and/or roles authorized to approve emergency changes, 3) protocols for reviewing emergency changes to determine if they were truly emergencies and not attempts to circumvent normal change management procedures, and 4) protocols for testing emergency changes to ensure related risks are properly managed.

☐ **Change Advisory Board:** The organization establishes a change advisory board (CAB) that provides perspectives on changes to the Change Manager. As an adjunct to the CAB, the organization establishes an emergency committee (CAB/EC) that supports change management in urgent scenarios.

☐ **Service Development Life Cycle (SDLC):** The organization defines and enforces standards around the creation of new services and service updates. The SDLC covers: 1) the collection and documentation of requirements; 2) design of the new system or update; 3) development procedures, including development standards; 4) testing protocols; 5) deployment into production of new services and updates; 6) requirements for services in production; 7) requirements for service maintenance; and 8) standards for decommissioning of services.

☐ **Rules of Behavior:** The organization establishes and makes readily available to all relevant staff a set of rules that describes their responsibilities and expected behavior with regard to change management. The organization receives signed acknowledgement from users indicating that they have read, understand, and agree to abide by the rules of behavior, before authorizing access to development and production systems.

☐ **Enforcement:** The organization defines a disciplinary process for employees that flout change management controls. To ensure change management policies are upheld by both internal employees and third parties, management defines disciplinary procedures for: 1) employees, 2) contractors, and 3) vendors.

Management Controls

Communications

Management actively oversees policies and processes related to IT product and service changes and related risks.

Description

- ☐ **Change Communication Plan:** The organization develops, disseminates, and enforces a change communication plan to inform staff stakeholders about the nature and impact of potential changes. The plan includes: 1) a formal, documented communication policy that addresses communication purpose, scope, roles, responsibilities, schedules, and compliance; 2) formal, documented procedures for communication; and 3) procedures for evaluating and responding to staff feedback throughout the project process. Designated officials within the organization review and approve the plan.
- ☐ **Stakeholder Analysis:** The organization: 1) identifies all staff who are involved in or stand to be impacted by a change or project, 2) categorizes stakeholders into communication groups, and 3) analyzes stakeholder expectations for communication
- ☐ **Communication Approval:** The organization specifies how communications should be generated and approved, including allocation of approval authority only to personnel formally authorized by management
- ☐ **Communication Record Retention:** The organization retains a record of all change-related communications

Procurement (System and Service[6] Acquisition)

Since all procurement implies some degree of change, procurement controls ensure that 1) participants in purchasing processes consider change-related risks before committing to purchase, and 2) all stakeholders in purchasing are aware of changes to procurement approval processes when they occur.

Description

- ☐ **System and Service Acquisition Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates polices and procedures for the procurement of IT products and services that addresses: 1) application of change management policies and procedures to acquisitions, and 2) the need for an impact assessment to analyze the ramifications of a requested change related to new or existing, software or services
- ☐ **Contract and Purchase Order Change Management:** The organization develops, disseminates, and periodically reviews/updates policies and procedures for making changes to existing purchase orders and contracts
- ☐ **System and Service Acquisition Approval:** The organization specifies how purchase requests should be processed and approved, including designation of purchase authority to personnel formally authorized by management
- ☐ **Notification to Vendors of Procurement Process Changes:** Vendors are notified of changes to procurement policies; for example, if the purchasing organization stops accepting verbal orders and begins requiring purchase orders
- ☐ **Procurement Training:** Personnel receive formal training on procurement policies and procedures

[6] According to the ITIL definition of service, configuration items can include hardware, software, people, facilities, services, documentation, and other technical and non-technical components that contribute to workable IT processes. System specifically relates to hardware and software and is used here to clearly differentiate procurement of IT products from procurement of services, such as outsourced application hosting, etc.

Operational Controls

Operational controls ensure the effective performance of the change management program. In general, operational controls assess whether:

- Controls exist to meet regulatory requirements
- Rules and requirements exist and are documented
- Staff performance appraisals are completed regularly
- Supervisory review of key management reports and operating results occurs regularly

Operational controls for change management include:

Awareness and Training

Organizations must ensure that managers and users of IT services are made aware of 1) risks associated with changes to IT systems; and 2) laws standards, policies, and procedures that govern change management. Moreover, management must ensure that organizational personnel have adequate training to meet change management objectives.

	Description
☐	**Change Management Awareness and Training Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a documented change management awareness and training policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) procedures for the implementation of change management awareness and training, as well as related security awareness and training controls
☐	**Change Management Awareness:** The organization ensures that all employees (including managers and senior executives) are made aware of change management awareness materials before gaining access to information systems
☐	**Change Management Training:** The organization identifies personnel whose job roles empower them to make significant changes to IT systems and services, documents their roles and responsibilities, and provides appropriate information change management training before authorizing access to information systems
☐	**Training Records:** The organization documents change management training activities at the individual level
☐	**Training Change Management:** The organization ensures that changes to training and awareness processes and programs adhere to general change management policies

Operational Controls

Change Management

Organizations The organization ensures that change requests are 1) registered, seen and approved by proper authorities; and 2) supported to a degree that allows management to appropriately evaluate risk associated with the change.

Description

- ☐ **Change Request Template:** The organization develops, disseminates, and periodically reviews/updates a change request template that documents a description and status of the change request. The change request template should contain: 1) date of request submission; 2) date of managerial review; 3) intended impact of the change; 4) potential risks associated with the change; 5) disposition of the review (approved, rejected, etc.); and 6) current status of the change (also reflecting the status of an associated project plan, if appropriate)
- ☐ **Change Request Log:** The organization maintains a log of all change requests. The log records information required by the change request template.
- ☐ **Review and Approval Process:** All IT service, process, and product changes are submitted and reviewed in written format. At least one appropriate manager, as defined by the organization, reviews every change request. The change approval authority reviews requests with the change owner prior to approving any change. Approval authorities notify change requestors of change acceptance or rejection.
- ☐ **Change Evaluation:** Management reviews change requests for: 1) business justification (cost vs. benefit); 2) technical feasibility; 3) project budget impact; 4) operating budge impact, both for the IT department and other affected departments; 5) project timeline impact; 6) information security impact; 7) compliance impact; 8) impact on other planned functionality related to the project; 9) impact of any delay or expedition of the change; and 10) historical precedence (whether the change has been previously attempted and the outcome of that effort)
- ☐ **Post-Implementation Reviews:** Management defines a policy, procedures, a timeline, and roles for post-implementation change reviews. The timeline for a change review is generally at least 30 days after the implementation of a change. The goal of the review is to determine the success or failure of a change, specifically: 1) Whether the change delivered the expected outcome, and 2) whether any incidents or problems occurred as a result of the change.
- ☐ **Periodic System, Product, and Service Audits:** The organization periodically audits IT systems and services to identify any deviations from approved conditions. If audits reveal unauthorized changes, the organization performs an investigation to determine the root causes of the changes and takes steps to correct any staff issues or control deficiencies revealed by the audit.

Segregation of Duties

Segregation of duties controls prevent IT staff from posting unauthorized changes to development, production, and testing environments. In smaller IT environments, where staffing limitations prevent complete segregation of duties, management should instill compensating controls that meet commensurate control objectives.

Description

- ☐ **Control of Changes to Source Code:** In order to control source code changes, managers establish controls to prohibit access to the source code repository by: 1) test engineers and test administrators, 2) database administrators, 3) system administrators, 4) IT operations personnel
- ☐ **Role Prohibitions:** Management establishes controls to prohibit developers from also acting as: 1) system administrators, 2) security administrators, 3) database administrators, and 4) test engineers and test administrators
- ☐ **Compensating Controls:** If staff limitations prevent full segregation of duties, management defines compensating controls that meet the goal of protecting development, testing, and production environments from unreviewed changes

Operational Controls

Protection of Development Environments

Change control must be strictly enforced in development environments, where tight deadlines, complex projects, and high pressures can facilitate mistakes and unauthorized changes. Organizations must protect the integrity of IT services, retain information about application versions, and track all changes to source code.

	Description
☐	**Integrity of the Development Environment:** The development environment is separate from test and production environments
☐	**Access to Development Environments:** The organization ensures that access to the source code repository is formally controlled through documentation requiring relevant management approval
☐	**Version Control:** The organization ensures that serial versions of software are tracked and noted by: 1) a check-in, check-out procedure, and 2) incremental versions of software are denoted by unique names or version numbers, generally assigned in increasing order
☐	**Source Code Audits:** Procedures exist for auditing the source code control system to verify that all activity surrounding the source code repository can be accounted for
☐	**Change Metadata:** The organization retains metadata about every change, including: 1) date of change, 2) the individual who implemented the change, 3) any new software version number associated with the change, and 4) the nature of the change
☐	**Third Party Code:** The organization manages the impact of third-party development by: 1) ensuring that third-party developers follow standard access management protocol, including unique logins, 2) establishing a "quarantine" environment for third-party code, and 3) separately testing third-party code for quality and security issues prior to releasing the code into development or production environments

Protection of Test Environments

Organizations must be able to protect the integrity of IT services through efficient and effective testing.

	Description
☐	**Integrity of the Test Environment:** The test environment is separate from development and production environments
☐	**Access to Test Environments:** The organization ensures that access to test environments is formally controlled through documentation requiring relevant management approval
☐	**Segregation of Duties:** The organization enforces segregation of duties sufficient to protect the test environment. Developers and production personnel cannot create or change access privileges to test environments
☐	**Change Management:** The organization ensures that changes to test environments follow defined change management procedures such that testing is performed on systems operating within known parameters
☐	**Test Environment Audits:** Procedures exist for auditing the test systems to verify that they do match defined build criteria
☐	**Change Metadata:** The organization retains metadata about every change, including: 1) date of change, 2) the individual who implemented the change, 3) request for change identifiers, and 4) the nature of the change

Operational Controls

Protection of Production Environments

Change control must be strictly enforced in production environments, where tight deadlines, complex projects, and high pressures can facilitate mistakes and unauthorized changes. Organizations must be able to protect the confidentiality, integrity and availability of production systems.

Description

- ☐ **Integrity of the Production Environment:** The production environment is separate from test and production environments
- ☐ **Access to Production Environments:** The organization ensures that access to test environments is formally controlled through documentation requiring relevant management approval
- ☐ **Segregation of Duties:** The organization enforces segregation of duties sufficient to protect the production environment. Developers and test personnel cannot create or change access privileges to production environments.
- ☐ **Change Management:** The organization ensures that changes to test environments follow defined change management procedures such that testing is performed on systems operating within known parameters
- ☐ **Production Environment Audits:** Procedures exist for auditing the production systems, in order to verify that they do match defined build criteria
- ☐ **Change Metadata:** The organization retains metadata about every change, including: 1) date of change, 2) the individual who implemented the change, 3) request for change identifiers, and 4) the nature of the change.

Personnel Security

Compliance and risk management programs must consider not only how technology enables change management controls, but how employees interact with technical controls, enact policies, and implement procedures.

Description

- ☐ **Personnel Screening:** The organization screens prospective contractors and employees through interviews and performs criminal and employment background checks prior to engagement
- ☐ **Personnel Termination:** Management ensures that, upon any individual's employment termination, voluntary or involuntary: 1) system administrators revoke the individual's access to all systems, and 2) the individual cannot effect further changes or participate in a change management process
- ☐ **Personnel Transfers:** The organization promptly processes employee transfers to ensure that: 1) system access and prohibitions reflect changes to job roles and responsibilities, and 2) change management roles and responsibilities reflect changes to job roles and responsibilities
- ☐ **Job Descriptions:** The organization formally documents staff responsibility for an effective control environment. Job descriptions include: 1) a requirement to comply with change management policies and procedures, and 2) affirmation of disciplinary action in cases of noncompliance with change management policies and procedures
- ☐ **Third Party Change Management Oversight:** The organization contractually requires third parties to adhere to change management controls. The organization has access to documentation demonstrating control adherence.

Operational Controls

Physical and Environmental Protection

Environmental security—including physical access to machinery and changes to the physical environment that might impact system performance—is a critical, but often-neglected, facet of change management. Organizations must take steps to ensure that technical security and change management controls are not undermined by weak physical security controls.

Description

- ☐ **Physical and Environmental Protection Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, physical and environmental protection policy that addresses purpose, scope, roles, responsibilities, and compliance, and 2) formal, documented procedures to facilitate the implementation of the physical and environmental protection policy and associated physical and environmental protection controls.
- ☐ **Physical Access Authorizations:** The organization develops and keeps current lists of personnel with authorized access to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and issues appropriate authorization credentials (e.g., badges, identification cards, smart cards). Designated officials within the organization review and approve the access list and authorization credentials.
- ☐ **Physical Access Control:** The organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. The organization also controls access to areas officially designated as publicly accessible, as appropriate, in accordance with the organization's assessment of risk.
- ☐ **Access Control for Transmission Medium:** The organization controls physical access to information system transmission lines carrying unencrypted information to prevent eavesdropping, in-transit modification, disruption, or physical tampering
- ☐ **Monitoring Physical Access:** The organization monitors physical access to information systems to detect and respond to incidents
- ☐ **Visitor Control:** The organization controls physical access to information systems by authenticating visitors before authorizing access to facilities or areas other than areas designated as publicly accessible
- ☐ **Access Logs:** The organization maintains a visitor access log to facilities (except for those areas within the facilities officially designated as publicly accessible) that includes: 1) name and organization of the person visiting, 2) signature of the visitor, 3) form of identification, 4) date of access, 5) time of entry and departure, 6) purpose of visit, and 7) name and organization of person visited. Designated officials within the organization review the access logs after closeout.
- ☐ **Power Equipment and Power Cabling:** The organization protects power equipment and power cabling for the information system from damage and destruction
- ☐ **Delivery and Removal:** The organization controls information system-related items (hardware, firmware, software) entering and exiting the facility and maintains appropriate records of those items
- ☐ **Alternate Work Site:** Individuals within the organization employ appropriate information physical security controls at alternate work sites
- ☐ **Changes to Physical and Environmental Services:** Changes to the physical and environmental protection services and controls adhere to change management policies

Operational Controls

Contingency Planning

A risk management approach to change management should facilitate not only successful changes, but mitigation of risk in the event of change failure. In some cases, contingency plans include resources at remote sites. And in all cases, plans should consider the potential impact of differences between primary and contingency technologies, staff, and facilities on service operation and performance.

Description

- ☐ **Contingency Plan:** The organization develops, documents, and implements a contingency plan that reduces the risks and costs associated with failed change implementations. The plan identifies roles, responsibilities, policies, and procedures associated with contingency responses. Designated officials within the organization review and approve the plan.
- ☐ **Rollback Plan:** The organization develops a rollback plan and procedures that allow developers to revert to a previous version of software if an update or new installation fails. Management periodically audits the rollback plan and procedures to ensure that older software versions implicated in the rollback plan are compatible with existing systems.
- ☐ **Contingency and Rollback Plan Updates:** The organization periodically reviews contingency and rollback plans and revises them to address system/organizational changes or problems identified during previous plan implementation or IT control assessments
- ☐ **Synchronization of IT Operations and Sites:** The organization's change management procedures ensure that the production and contingency sites are managed such that the ability to fail over in the planned manner is not at risk
- ☐ **Changes to Contingency Plans:** The organization's contingency plans are governed by change management to ensure that impacts are properly understood and addressed

Configuration Management

Management should consider how variables in application options, user access, and performance setting impact IT service offerings. Even apparently minor configuration changes can have major (and sometimes unintended) consequences.

Description

- ☐ **Configuration Change Management:** The organization ensures that configuration changes adhere to general change management policies. If configuration management services are automated, the software is configured to conform to organizational change management controls.
- ☐ **Configuration Authority:** The organization limits authority for configuration changes to specific staff roles. All configuration changes are performed by authorized staff.
- ☐ **Configuration Change Monitoring:** Management reviews any configuration changes to assess impact on the broader systems and control environment
- ☐ **Periodic Configuration Audits:** The organization conducts audits to determine whether configurations have "drifted" from their documented state; for example, in the event of unauthorized configuration changes. If audits reveal unauthorized changes, the organization performs an investigation to determine the root causes of the changes and takes steps to correct any staff issues or control deficiencies revealed by the audit.

Operational Controls

Maintenance

Standard application maintenance often involves or indicates required changes. In some cases, however, application updates and regular maintenance may fall to employees outside of the core development group; for example, if business users are allowed to install updates issued from an application vendor's servers. Management and auditors should consider all sources and types of software maintenance when developing change management controls.

Description

- ☐ **Maintenance Change Management:** The organization ensures that maintenance that results in configuration changes adheres to general change management policies. If maintenance services are automated, the software is configured to conform to organizational change management controls.

System and Information Integrity

In general, organizations should implement controls that 1) identify, report, and correct information and information system flaws in a timely manner; 2) protect systems and data from malicious code; and 3) implement protection measures in response to security alerts and advisories. Although some protection measures, like patch updates or antivirus software updates, might be implemented in an atmosphere of high pressure or anxiety, organizations must balance the need for urgent action against the risk that an untested system update (for example) will negatively impact system performance or business processes.

Description

- ☐ **Security and Protection Change Management:** The organization ensures that information and system protection processes adheres to general change management policies. If protective services and updates are automated, the software is configured to conform to organizational change management controls.
- ☐ **Design of Change Management Controls:** Change management policies and procedures are designed to mitigate risks associated with both human error and malicious software code
- ☐ **Alignment of Information Integrity and Change Management:** Organizations ensure that: 1) change management policies and procedures align with other policies and procedures designed to protect system and information integrity, and 2) information protection processes do not undermine change management controls

Media Protection

In general, organizations should implement controls that 1) identify, report, and correct information and information system flaws in a timely manner; 2) protect systems and data from malicious code; and 3) implement protection measures in response to security alerts and advisories. Although some protection measures, like patch updates or antivirus software updates, might be implemented in an atmosphere of high pressure or anxiety, organizations must balance the need for urgent action against the risk that an untested system update (for example) will negatively impact system performance or business processes.

Description

- ☐ **Media Protection Change Management:** The organization ensures that media protection processes adhere to general change management policies. If protective services and updates are automated, the software is configured to conform to organizational change management controls.

Operational Controls

Incident Response

Incident response controls generally ensure that an organization establishes an operational incident handling capability for information systems that includes adequate preparation, detection, analysis, containment, recovery, and user response activities; and that the organization tracks, documents, and reports incidents to appropriate organizational officials and/or authorities. Like information integrity processes, incident response can carry a sense of urgency that tempts both staff and management to autonomously circumvent change management controls.

	Description
☐	**Incident Response Change Management:** The organization ensures that incident response processes adhere to general change management policies
☐	**Emergency Change Management Procedure:** The organization develops, documents, and implements an emergency change management procedure designed to balance expediency and risks during incident response

Technical Controls

Technical controls ensure that change management enactment is effective and efficient. Technical controls include:

Access Control

Controlling access to information systems is a critical component of change management. Organizations must limit information system access to authorized users, processes acting on behalf of authorized users, or devices (including other information systems) and to the types of transactions and functions that authorized users are permitted to exercise.

	Description
☐	**Access Control Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, access control policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the access control policy and associated access controls
☐	**Account Management:** The organization manages information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization reviews information system accounts.
☐	**Information Flow Enforcement:** The information system enforces assigned authorizations for controlling the flow of information within the system and between interconnected systems in accordance with applicable policy
☐	**Separation of Duties:** The information system enforces separation of duties through assigned access authorizations
☐	**Least Privilege:** The information system enforces the most restrictive set of rights/privileges or accesses needed by users (or processes acting on behalf of users) for the performance of specified tasks
☐	**Unsuccessful Login Attempts:** The information system enforces a limit on consecutive invalid access attempts by a user during a defined time period. If the limit is exceeded, the information system automatically locks out the user for a defined period of time.
☐	**Previous Logon Notification:** The information system notifies the user, upon successful logon, of the date and time of the last logon, and the number of unsuccessful logon attempts since the last successful logon
☐	**Concurrent Session Control:** The information system limits the number of concurrent sessions for any user to a defined number of sessions

Technical Controls

Access Control *(continued)*

	Description
☐	**Session Lock:** The information system prevents further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures
☐	**Session Termination:** The information system automatically terminates a session after a defined period of inactivity
☐	**Supervision and Review:** The organization supervises and reviews the activities of users with respect to the enforcement and usage of information system access controls
☐	**Permitted Actions without Identification or Authentication:** The organization identifies and documents specific user actions that can be performed on the information system without identification or authentication
☐	**Automated Marking:** The information system marks output using standard naming conventions to identify any special dissemination, handling, or distribution instructions
☐	**Automated Labeling:** The information system appropriately labels information in storage, in process, and in transmission
☐	**Remote Access:** The organization documents, monitors, and controls all methods of remote access (e.g., dial-up, wireless, Internet) to the information system. Appropriate organization officials authorize each remote access method for the information system and authorize only the necessary users for each access method.
☐	**Wireless Access Restrictions:** The organization: 1) establishes usage restrictions and implementation guidance on the use of wireless technologies; and 2) documents, monitors, and controls wireless access to the information system. Appropriate organizational officials authorize the use of wireless technologies.
☐	**Access Control For Portable And Mobile Devices:** The organization: 1) establishes usage restrictions and implementation guidance for portable and mobile devices; and 2) documents, monitors, and controls device access to organizational networks. Appropriate organizational officials authorize the use of portable and mobile devices.
☐	**Personally Owned Information Systems:** The organization restricts the use of personally owned information systems for official business involving the processing, storage, or transmission of federal information
☐	**Access Control Change Management:** The organization ensures that access control processes adhere to general change management policies and that automated services are configured to conform to organizational change management controls

Identification and Authentication

In order to control access to information systems, organizations must identify information system users, processes acting on behalf of users, or devices and authenticate (or verify) the identities of those users, processes, or devices, as a prerequisite to allowing access to organizational information systems.

	Description
☐	**Identification and Authentication Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, identification and authentication policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the identification and authentication policy and associated identification and authentication controls
☐	**User Identification and Authentication:** The information system uniquely identifies and authenticates users (or processes acting on behalf of users)

Technical Controls

Identification and Authentication *(continued)*

	Description
☐	**Device Identification and Authentication:** The information system identifies and authenticates specific devices before establishing a connection
☐	**Identifier Management:** The organization manages user identifiers by: 1) uniquely identifying each user, 2) verifying the identity of each user, 3) receiving authorization to issue a user identifier from an appropriate organization official, 4) ensuring that the user identifier is issued to the intended party, 5) disabling user identifier after a defined period of inactivity, and 6) archiving user identifiers
☐	**Authenticator Management:** The organization manages information system authenticators (e.g., tokens, PKI certificates, biometrics, passwords, key cards) by: 1) defining initial authenticator content; 2) establishing administrative procedures for initial authenticator distribution, for lost/compromised, or damaged authenticators, and for revoking authenticators; and 3) changing default authenticators upon information system installation
☐	**Authenticator Feedback:** The information system provides feedback to a user during an attempted authentication and that feedback does not compromise the authentication mechanism
☐	**Cryptographic Module Authentication:** for authentication to a cryptographic module, the information system employs authentication methods that meet standards adopted by the organization
☐	**Identification and Authentication Change Management:** The organization ensures that access control processes adhere to general change management policies and automated services are configured to conform to organizational change management controls

Change Testing

The need for testing and approval of all code changes is a central tenet of change management. The primary purpose of testing controls is to reduce the risk that changes to source code will adversely affect production systems.

	Description
☐	**Testing Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented application testing policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the testing policy and associated controls
☐	**Testing Change Management:** The organization ensures that testing processes adhere to general change management policies and automated services are configured to conform to organizational change management controls
☐	**Alignment of Testing, Development, and Production Environments:** The organization ensures that the testing environment is congruent with production and development environments to a degree that applications perform similarly in both testing and production environments
☐	**Coordination of Changes and Testing Schedules:** The organization creates a Forward Schedule of Change (FSC) for the test environment(s), so that changes do not adversely impact testing

Technical Controls

Audit and Accountability

Organizations must: 1) create, protect, and retain information system audit records to the extent needed to enable the monitoring, analysis, investigation, and reporting of unlawful, unauthorized, or inappropriate information system activity; and 2) ensure that the actions of individual information system users can be uniquely traced to those users so they can be held accountable for their actions.

Description

- ☐ **Audit and Accountability Policy and Procedures:** The organization develops, disseminates, and periodically reviews/updates: 1) a formal, documented, audit and accountability policy that addresses purpose, scope, roles, responsibilities, and compliance; and 2) formal, documented procedures to facilitate the implementation of the audit and accountability policy and associated audit and accountability controls
- ☐ **Auditable Events:** Change management procedures are designed such that they are auditable
- ☐ **Audit Records Policy and Procedures:** Audit policies and procedures specify: 1) what change management documentation is to be retained, 2) how long change management documentation must be retained, 3) methods of short-term storage and space requirements, 4) method of long-term archiving and space requirements, 5) security considerations for audit records, and 6) the proper method of destruction for change management records.
- ☐ **Content of Audit Records:** The information system captures sufficient information in audit records to establish what change events occurred, the sources of the events, and the outcomes of the events
- ☐ **Audit Storage Capacity:** The organization allocates sufficient audit record storage capacity and configures auditing to prevent such capacity being exceeded
- ☐ **Audit Processing:** In the event of an audit failure or audit storage capacity being reached, the information system alerts appropriate organizational officials and takes predetermined actions
- ☐ **Audit Monitoring, Analysis, and Reporting:** The organization at least annually reviews/analyzes audit records for indications of inappropriate or unusual activity, investigates suspicious activity or suspected violations, reports findings to appropriate officials, and takes necessary actions
- ☐ **Audit Reduction and Report Generation:** The information system provides an audit reduction and report generation capability
- ☐ **Date and Time Stamps:** The information system provides date and time stamps for use in audit record generation
- ☐ **Protection of Audit Information:** The information system protects audit information and audit tools from unauthorized access, modification, and deletion
- ☐ **Non-repudiation:** The information system provides the capability to determine whether a given individual took a particular action (e.g., instigated a configuration change or created information)
- ☐ **Audit Retention:** The organization retains audit logs for a predetermined period to support after-the-fact investigations of change incidents and to meet regulatory and organizational information retention requirements
- ☐ **Audit and Accountability Change Management:** The organization ensures that audit and accountability processes adhere to general change management policies and automated services are configured to conform to organizational change management controls

Audit Reporting

During the reporting phase, management and the board of directors receive formal feedback from the audit team. This knowledge transfer should be an open and transparent process.

Almost every audit identifies opportunities for improvement. The primary goal of management and auditors should be to address critical issues first, followed by important issues. Both management and auditors should work to ensure that, whatever action plans they agree to, the goals are achievable and beneficial to the organization.

During the reporting phase, management must determine which corrective actions it will implement and when, based on audit findings. Mangers will provide oversight and support to ensure the timely resolution of found issues. Although the audit team may make recommendations based on its assessments of risks and consequences, it cannot make or dictate managerial decisions.

The following are typical steps an audit team takes to confirm and release the audit results.

- ☐ Auditors debrief management, formally discussing significant audit findings and conclusions before they issue the final audit report
- ☐ Managers receive a written draft report from auditors
  - — The report communicates audit results clearly and precisely
  - — Results are presented in an unbiased tone, noting where management has taken actions to correct deficiencies and acknowledging good performance
- ☐ Management and auditors discuss the draft report
- ☐ Management provides feedback on the draft report
- ☐ Auditors review managerial comments and action plan(s)
- ☐ Auditors finalize and distribute the final audit report
- ☐ Auditors close out the internal audit project and plan any necessary follow-up efforts regarding management's action plans

Auditors might also choose to communicate some audit findings that might be useful for change management efficiency and effectiveness, but do not warrant inclusion in the formal report. This type of communication should be documented, if only as a note in audit findings that the topic has been verbally discussed.

Preparing for an Audit

A well-managed business unit or governance program includes robust plans, procedures, goals, objectives, trained staff, performance reporting, and ongoing improvement efforts. The internal audit team looks for evidence that the business unit and governance program is well organized and well managed. The change management program must also specifically and traceably mitigate risks related to key business objectives. Managerial preparation should mainly be routine, day-to-day practices.

Management's ultimate goal in the audit process is not to make auditors happy, but rather to demonstrate that change management efforts meet the demands of the CEO, board of directors, regulators, and investors. Likewise, auditors' requests should be aligned with these overarching needs; that is, to support responsible program performance within a sound, ethical business environment.

While the audit is in the planning phase, management should proactively work with the audit team and "educate" the auditors. As a rule, managers should provide constructive input on the evaluation methodology before audit management approves it. Expectations are a two-way street: management must help auditors ensure that audit expectations are aligned and that participants understand each other.

Prior to the audit, managers should collect the information and documentation necessary to demonstrate how well they manage their operations in concert with the overall organizational business objectives. They should be prepared to provide auditors with evidence of well-managed change management efforts and results. This might include documentation of change management plans, supporting budgets, policy and procedure manuals, assignments of responsibilities (such as up-to-date job descriptions), results reporting and other trending information, and finally, any other relevant guidance (to management and staff) that demonstrates a "well-run" and performing program.

In selecting documentation, management should not try to overload the audit team with information, but to provide genuine insight into how the change management program is run and how well it is doing. A change management periodic risk assessment and organizational business impact analysis (BIA) are two key management efforts to share with auditors.

Other steps management should take to prior to the audit:

- ☐ Learn early and contribute often to the internal audit goals, objectives, purpose, approach, and procedures (audit tests). In particular, setting an appropriate purpose and the audit approach are the two most important elements of every successful audit.
- ☐ Discuss with audit management the evaluation criteria and standards and how the audit will actually be conducted, in order to ensure that you'll receive a quality audit. Ask whether they audit in accordance with international standards for the professional practice of internal auditing.
- ☐ Learn who is on the audit team and their qualifications, talents, and motivations. The audit team exists to help make your operations more efficient and effective, but they are also individuals with strengths and weaknesses common to many employees. It pays to know the experience of your auditors, whether they're rookies or veterans (and perhaps to push for the latter). Showing an interest in their work can also influence and increase the benefits from the audit—within reason. At the end of the day, auditors still need to be independent and objective.

Throughout its discussion with the audit team prior to the audit, management should try to strike a balance between influence and deference. Managers should neither yield entirely to the audit team nor micromanage its efforts.

Communicating with Auditors

Like any interaction between people, but particularly in the work environment, a professional and trusting relationship is a strong precursor to successful collaboration.

When managers interact with the auditors in a professional manner, they tell the audit team that its function is respected and supported. Likewise, lackadaisical efforts by managers and staff reflect poorly on the business unit or process, its capabilities, and its performance. Managers should also expect professional interaction from the audit team and push back whenever they see an exception to this practice.

To contribute to a successful and accurate audit report, managers should be receptive to auditor observations and the audit team's recommendations. Managers should also be firm when discussing anything they see as incorrect, in order to ensure there are no misunderstandings.

Finally, always remember: managers, not auditors, are responsible for defining and implementing solutions to issues found in the audit. Thus, it is in everyone's best interest to have a cooperative, collaborative audit process that respects the independence and discretion of all participants. Auditors should listen to management. And for its part, management should encourage staff to be open and honest with auditors.

APPENDIX A—
Change Management Resources

British Educational Communications and Technology Agency (BECTA)Framework for ICT [information and communications technology] Technical Support
http://www.becta.org.uk/tsas

Institute of Internal Audit (IIA) Guide 2: Change and Patch Management Controls: Critical for Organizational Success
http://stage.theiia.org/guidance/technology/gtag/gtag2/

IT Process Institute Control Performance Benchmarking Study
http://www.itpi.org/home/controls_benchmark.php

IT Process Institute Visible Ops Handbook: Implementing ITIL in 4 Practical and Auditable Steps
http://www.itpi.org/home/visibleops2.php

National Institute of Standards and Technology (NIST) Special Publication 800-53–Recommended Security Controls for Federal Information Systems
http://csrc.nist.gov/publications/nistpubs/800-53/SP800-53.pdf (PDF)

Office of Government Commerce (OGC) Best Management Practice for Project, Programme, Risk and Service Management
http://www.best-management-practice.com/officialsite.asp

Office of Government Commerce (OGC) IT Infrastructure Library (ITIL)
http://www.itil.co.uk/

Microsoft Microsoft Operations Framework (MOF) Service Management Functions (SMF)
http://www.microsoft.com/technet/itsolutions/cits/mo/smf

Research Sponsors

Solidcore

Solidcore is a leading provider of change control for critical systems. Organizations worldwide trust Solidcore to improve service availability and lower the costs of complying with Payment Card Industry (PCI) and Sarbanes-Oxley (SOX) standards. Solidcore enables customers to automate the validation of controls and eliminate the expensive, time consuming and error-prone manual processes that consume IT resources.

As the industry's first and only solution to automate the enforcement of change polices, Solidcore S3 Control allows organizations to prevent and alert rather than detect and remediate. Solidcore uses real-time change detection capabilities along with automated, highly-accurate change reconciliation to provide an automated way of validating changes against authorizations. Out-of-process changes, such as emergency fixes, can be automatically documented and reconciled for easier audit-ability.

Solidcore's partnerships with industry leaders such as Opsware, BMC, HP, and IBM help make it the preferred choice for ensuring compliance and change control across the enterprise. As an Opsware partner, customers can integrate Solidcore's S3 Control software with the Opsware System 6 Solutions suite to proactively enforce Opsware as an authorized change agent. Solidcore's integrations with BMC Remedy, HP Service Center and IBM Tivoli also enable customers to drive all change through those approved changed management processes, and effectively eliminate ad hoc change.

Solidcore also provides change control for embedded systems and is used by major device manufacturers to securely leverage open systems to meet their business requirements. Solidcore is also a Gold-level partner in the Microsoft Windows Embedded Partner Program. For more information, please visit **http://www.solidcore.com**.

Tripwire

Tripwire delivers immediate value to the business by assuring continuous operational, regulatory and security compliance across the dynamic data center. As the clear leader of the configuration audit and control market, Tripwire ensures the continuous control of configuration activity in real-time across the IT infrastructure, automatically correlating configuration activity with policies and generating actionable reports.

- Continuous Compliance
  Tripwire provides a holistic and continuous view of security, risk and compliance across the IT infrastructure, so users can take a proactive approach to assessing, controlling and reporting compliance.

- Configuration Assessment
  Only Tripwire integrates configuration assessment functionality with change management to automatically validate configuration settings against policy.

- Real-Time, Tunable Change Detection
  Tripwire is the only solution to combine event-driven real time harvesting with detailed 'scan-based' change detection, delivering all the advantages of each approach in one system of record and unmatched flexibility.

- Integration
  Tripwire reconciles change data with other management systems. Certified integrations with the leading change management and service desk systems – like BMC, CA and HP – plus an open API for customer integrations, provide the most comprehensive configuration audit and control solution available.

Tripwire, Inc. is the recognized leader of configuration audit and control solutions, serving over 5,700 enterprises worldwide. Global enterprises rely on Tripwire to strengthen their compliance and security, reduce unplanned work, increase availability, and accelerate success with CMDB initiatives. Tripwire is headquartered in Portland, OR with offices in the UK and Japan. For more information, visit: **http://www.tripwire.com**.

ABOUT THE AUTHORS

George Spafford

George Spafford is Principal Consultant with Pepperweed and an experienced practitioner in business and IT operations. He is a prolific author and speaker, and has consulted and conducted training on regulatory compliance, IT Governance, and process improvement in the U.S., Australia, New Zealand and China. Publications include co-authorship of "The Visible Ops Handbook." George Spafford's Daily News is read by over 2,500 subscribers, including high-level executives from Fortune 500 and leading international companies. George holds an MBA from Notre Dame, a BA in Materials and Logistics Management from Michigan State University and an honorary degree from Konan Daigaku in Japan. He is a Certified Information Systems Auditor (CISA) and holds ITIL Practitioner Release and Service Manager certifications. George is a current member of ISACA, the IIA, and the IT Process Institute.

Dan Swanson, CMA, CIA, CISA, CISSP, CAP

Dan Swanson is a 25-year internal audit veteran who was most recently director of professional practices at the Institute of Internal Auditors. Prior to his work with the IIA, Swanson was an independent management consultant for over 10 years. Swanson has completed internal audit projects for more than 30 different organizations, spending almost 10 years in government auditing at the federal, provincial, and municipal levels, and the rest in the private sector, mainly in the financial services, transportation, and health sectors. The author of more than 100 articles on internal auditing and other management topics, Swanson is currently a freelance writer and management consultant with Seccuris.

Swanson led the writing of the OCEG internal audit guide for use in audits of compliance and ethics programs (www.oceg.org) and participated in the COSO small business task force efforts to provide guidance for smaller public companies regarding internal control over financial reporting (http://www.coso.org). Swanson is a regular columnist for Compliance Week and writes regularly for ITCI.

Series Editor: Cass Brewer
Editorial and Research Director,
IT Compliance Institute (ITCi)

If you have ideas for improving ITCi's IT Audit Checklists, please write editor@itcinstitute.com.