IT Service Delivery And Support Week Twelve

IT Auditing and Cyber Security

Fall 2016

Instructor: Liang Yao

Change Management

* Defining IT Change Management
* Change Management Key Controls
* Change Management Process
* Why IT Change and Patch Management are Important
* How IT Change and Patch Management Help Control IT Risks and Costs
* Effective IT Change Management Elements
* How to Verify IT Change and Patch Management Are Working?
* How to Reduce IT Change Risks?

Change Management

* What Internal Audit Should Do?
* Change Management Related Standards and Guidance
* Sample Change Management Audit Program
* Integrate Patch Management, Release Management and Configuration Management

Change Control: ISACA Definition

"All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes (including those to procedures, processes, system and service parameters) are logged, assessed and authorised prior to implementation and reviewed against planned outcomes following implementation. This assures mitigation of the risks of negatively impacting the stability or integrity of the production. "

The COBIT Acquire and Implement (AI) domain addresses good practices for systems development and maintenance. AI6 *Manage changes* specifically addresses change management.

Defining Change Management

* *"a set of process executed within the organization to manage the organization's IT department designed to manage the enhancements, updates, incremental fixes, and patches to production systems."* (GTAG – Change and Patch Management Controls: Critical for Organizational Success)
* E.g. Application code revision; System upgrades; Infrastructure changes.

Defining Change Management

What's the source of IT related changes???

Defining Change Management

* Change Management Scope - upgrades or updates to IT assets are identified for moving to production
  * Scope of Changes
    * ***Hardware:*** mainframes, servers, workstations, routers, switches, and mobile devices.
    * ***Software:*** operating systems and applications.
    * ***Information, data, and data structures:*** files and databases.
    * ***Security controls:*** antivirus software, firewalls, and intrusion protection/detection systems.
    * ***Processes, policies, and procedures.***
    * ***Roles/responsibilities:*** authorization, authority to act, and access controls.

Defining Change Management

* System and application maintenance
* Emergency changes
* Exclusion: changes occurs during the design and development phases
* Source of Change
  * External environment (e.g., competitive market, stakeholders/shareholders, changing risks).
  * Regulatory environment.
  * Business objectives, goals, strategies, requirements,
  * processes, and shifts in priorities.
  * Vendors (e.g., new products, upgrades, patches, and vulnerabilities).
  * Partners and suppliers.
  * Results of an audit, risk assessment, and other type of evaluation or assessment.
  * Operational problems.
  * Changes in performance or capacity requirements

Types of Changes in IT Operations & Change Categories

* **Types of Changes in IT Operations**
  * New installation
  * Replacement
  * Upgrade/Addition
  * Downgrade/Removal
  * Patches/hotfixes
  * Move/Relocation
* **Change Categories**
  * Standard
  * Minor
  * Major
  * Significant

Change Management Controls

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

Change Management Processes

* Identifying the need for the change.
* Preparing for the change.
  * Documenting the change request in detail.
  * Documenting the change test plan.
  * Documenting a change rollback plan in the event of change failure.
  * Writing a step-by-step procedure that incorporates the change, test plan, and rollback plan.
  * Submitting the change procedure in the form of a change request.
* Developing the business justification and obtaining approvals.
  * Assessing the impact, cost, and benefits associated with the change request.
  * Reviewing and assessing the risks and impacts of the change request, including regulatory impacts.

Change Management Processes

* Authorizing the change request.
  * Authorizing, rejecting, or requesting additional information about the change request.
  * Prioritizing the change request with respect to others that are pending.
* Scheduling, coordinating, and implementing the change.
  * Scheduling and assigning a change implementer.
  * Scheduling and assigning a change tester.
  * Testing the change in a preproduction environment.
  * Communicating the change to stakeholders who likely will be affected.
  * Approving the change for implementation.
  * Implementing the change as requested.

Change Management Processes

* Verifying and reviewing the implemented change. (This is an often-overlooked critical step.)
  * Was the change successful?
  * Was the change process followed?
  * What was the variance between the planned and implemented change?
  * Were internal control, operations, and regulatory compliance requirements maintained?
  * What were the lessons learned that can be used to improve the process?
* Backing out the change (if unsuccessful).
* Closing the change request and communicating with the affected parties.
* Making agreed-to changes to the change management process.
* Publishing the change schedule.

Why IT Change Management are Important

A good change management can help an organization:

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

Key Risks Associated with Change Management

* Unauthorized business process changes being introduced into the operations
* Financial statements being materially misstated
* Unintended side effects
* Inconsistent processing results
* Changes not being recorded and tracked
* Emergency changes being implemented without adequate oversight, resulting in the introduction of erroneous processes, unauthorized business processes and inefficiencies
* Lack of priority management of changes
* Inability to respond effectively to emergency change needs

Key Risks Associated with Change Management (cont.)

* Additional access authorization not being terminated properly
* Unauthorized changes being applied, resulting in compromised security and unauthorized access to corporate information
* Failure to comply with compliance requirements
* Changes not being adequately prioritized or aggregated, resulting in lost productivity, late implementation of required changes, or redundancy
* Adverse effects on capacity and performance of the infrastructure
* System or application failure, resulting in lack of availability
* Reduced system availability
* Security intrusions
* Insufficient allocation of resources

Effective IT Change Management Elements

IT Management Needs to Know:

* What is being changed, why it is being changed, and when it is being changed.
* How efficiently and effectively changes are implemented.
* Problems that are caused by changes and the severity of the problems.
* Cost of the changes.
* Benefits the changes provide.
* Early and frequent involvement by management and end users to align IT changes with business needs.
* A defined, predictable, repeatable process with defined, predictable, repeatable results.
* Coordination and communication with constituents affected by changes.

Verify IT Change Management Effectiveness

* An documented change management process
* Identify controls in place in change management process. Are controls in place and being improved, or are they just being evaluated and deferred until “firefighting” subsides?
* Benefits from the change management process? Are there measurable benefits
* Number of outages caused by changes? Recurrence of the problem?
* How does IT monitor the effectiveness of the change management process?
* Indicators and measures
* What is the goal of our change management process?
* How disruptive is the patching process? Is patch management part of a defined, repeatable change and release process, or is it ad hoc, informal, and emergency-based?

Indicators & Symptoms

* Top five poor change management indicator
  * ***Unauthorized changes (Above zero is unacceptable.)***
  * ***Unplanned outages***
  * ***Low change success rate***
  * ***High number of emergency changes***
  * ***Delayed project implementations***

Indicators & Symptoms

* Unavailability of critical services and functions — even for short periods of time.
* Unplanned system or network downtime that halts execution of critical business processes, such as coordinating schedules with suppliers and responding to customer orders.
* Downtime on critical applications, databases, or Web servers that prevent users from performing their critical tasks.
* Negative publicity and unwanted board attention.

Indicators & Symptoms

* Majority of the IT organization's time is spent on operations and maintenance (>70 percent) instead of helping the business in deploying new capability.
* Failure to complete projects and planned work (due to high amounts of "firefighting" and unplanned work).
* IT management is being awakened in the middle of the night regarding problems.
* High IT staff turnover.
* Adversarial relationships between IT support staff, developers, and business customers (internal or external), usually over poor service quality or late delivery of functionality.
* High amounts of time required for IT management to prepare for IT audits and to remediate the resulting findings.

Indicators & Symptoms

* Changes authorized per week.
* Changes implemented per week.
* Number of unauthorized changes that circumvent the change process.
* Change success rate (percentage of actual changes made that did not cause an outage, service impairment, or an episode of unplanned work).
* Number of emergency changes (including patches).
* Percentage of patches deployed in planned software releases.
* Percentage of time spent on unplanned work.
* Percentage of projects delivered later than planned.

How to Reduce IT Change Risks?

* Create **tone at the top** motivating the need for a culture of change management across the enterprise that is supported by a declaration from IT management that the only acceptable number of unauthorized changes is zero. Preventive and detective controls can then be put in place to help achieve and sustain this objective, ensuring that all production changes can be reconciled with authorized work orders.
* Continually monitor the number of **unplanned outages**, which is an excellent indicator of unauthorized change and failures in change control.

How to Reduce IT Change Risks?

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

What Internal Audit Should Do?

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

What Internal Audit Should Do?

* Understanding the controls that are crucial to a solid IT change management approach:
  * Preventive.
    * Appropriate authorizations.
    * Separation of duties.
    * Supervision.
  * Detective.
    * Detection of unauthorized changes.
    * Monitoring of valid, objective change management metrics.
  * Corrective.
    * Post-implementation reviews.
    * Change information fed into early problem diagnosis steps.
* Keeping up to date on leading IT change and patch management processes and recommending that the organization adopt them.
* Demonstrating how management can reap the benefits of better risk management, greater effectiveness, and lower costs.
* Assisting management in identifying practical, effective approaches to IT change management.

Change Management Related Standards and Guidance

* Standards
  * Standard 2120: Risk Management
  * Practice Advisory 2120-1: Assessing the Adequacy of Risk Management Processes
  * Standard 2130: Control
  * Practice Advisory 2130-1: Assessing the Adequacy of Control Processes
  * Practice Advisory 2130-A1-1: Information Reliability and Integrity
* Guidance
  * GTAG 1: IT Controls
  * GTAG 3: Continuous Auditing: Implications for Assurance, Monitoring, and Risk Assessment
  * GTAG 9: Identity and Access Management
  * GTAG 17: IT Governance (pending publication)
  * Practice Guide, Auditing the Control Environment
  * Practice Guide, Assessing the Adequacy of Risk Management

AI6.1 *Change standards and procedures*

* Control objective—Set up formal change management procedures to handle in a standardized manner all requests (including maintenance and patches) for changes to applications, procedures, processes, system and service parameters, and the underlying platforms.
* Value drivers:
  * An agreed-upon standardized approach for managing changes in an efficient and effective manner
  * Changes reviewed and approved in a consistent and coordinated way
  * Formally defined expectations and performance measurements
* Risk drivers:
  * Inappropriate resource allocation
  * No tracking of changes
  * Insufficient control over emergency changes
  * Increased likelihood of unauthorized changes being introduced to key business systems
  * Failure to comply with compliance requirements
  * Unauthorized changes
  * Reduced system availability

AI6.2 *Impact assessment, prioritization and authorization*

* Control objective—Assess all requests for change in a structured way to determine the impact on the operational system and its functionality. Ensure that changes are categorized, prioritized and authorized.
* Value drivers:
  * An agreed-upon and standardized approach for assessing impacts in an efficient and effective manner
  * Formally defined change impact expectations based on business risk and performance measurement
  * Consistent change procedure
* Risk drivers:
  * Unintended side effects
  * Adverse effects on capacity and performance of the infrastructure
  * Lack of priority management of changes

AI6.3 *Emergency changes*

* Control objective—Establish a process for defining, raising, testing, documenting, assessing and authorizing emergency changes that do not follow the established change process.
* Value drivers:
  * An agreed-upon and standardized approach for managing changes in an efficient and effective manner
  * Formally defined emergency change expectations and performance measurement
  * Consistent procedure for emergency changes
* Risk drivers:
  * Inability to respond effectively to emergency change needs
  * Additional access authorization not terminated properly
  * Unauthorized changes applied, resulting in compromised security and unauthorized access to corporate information

AI6.4 *Change status tracking and reporting*

* Control objective—Establish a tracking and reporting system to document rejected changes, communicate the status of approved and in-process changes, and complete changes. Make certain that approved changes are implemented as planned.
* Value drivers:
  * An agreed-upon and standardized approach for managing changes in an efficient and effective manner
  * Formally defined expectations and performance measurement
  * Consistent change procedure
* Risk drivers:
  * Insufficient allocation of resources
  * Changes not recorded and tracked
  * Undetected unauthorized changes to the production environment

AI6.5 *Change closure and documentation*

* Control objective—Whenever changes are implemented, update the associated system and user documentation and procedures accordingly.
* Value drivers:
  * An agreed-upon and standardized approach for documenting changes
  * Formally defined expectations
  * Consistent change and documentation procedures
* Risk drivers:
  * Increased dependence on key individuals
  * Configuration documentation failing to reflect the current system configuration
  * Lack of documentation of business processes
  * Failure of updates for hardware and software changes

Change Management Audit Program

Sample Change Management Audit Program from ISACA

Related Topics

* Patch Management
* Release Management
* Configuration Management