Ia | INTERNAL AUDITOR

September 2011

IT Change Management

Auditors should provide assurance that the organization has a process in place to ensure that changes to the IT production environment don't disrupt business or cause security breaches.

Shannon Buckley, CIA, CISA, CGEIT, CPA
Senior Auditor
Bupa International Markets

Comedian Billy Crystal once said, “Change is such hard work.” In an IT environment change is particularly tricky. The implications of incorrectly implementing a change into an organization’s production system environment can lead to potential security breaches and result in negative publicity or regulatory sanctions if breaches occur. Moreover, organizations that lack a change management process run a significant risk that unauthorized changes may be introduced into the production environment.

A change management process is a formal set of procedures and steps that are set in place to manage all changes, updates, or modifications to hardware and software (systems) across an organization. Typically, the change management process should be formalized through a management-approved policy. From an internal audit perspective the policy should cover:

- *Scope of policy.* The scope should detail the types of change and systems for which the policy is applicable.
- *Authorization and approval.* All major changes should be authorized by the system owner before its implementation in a live environment. The policy should identify which changes are exempt from the change management process, but the exemption should be documented and approved.
- *Testing requirements.* All changes must be tested and approved by the users/system owner before migration into the production environment.
- *Segregation of duties.* The physical act of migrating the change should be performed by an independent person. Typically, this is completed by the change and release manager.

The auditor should provide assurance that a change management policy and framework are in place to ensure that all changes to production systems are managed consistently and formally.

Moreover, they should ascertain whether the organization educates users of the process on the various steps.

CHANGE MANAGEMENT PROCESS

The purpose of the change management process is to manage the scheduling of changes with minimum disruption to IT services. The goal of the process is to implement fault-free changes with minimal business impact. A definition of a change should be specified in the process. Typically, a change is any task or action that can alter the organization's IT production environment.

Step 1: Initiation

A change inquiry may be initiated by a user or a nominated business representative, who usually completes a form specifying the type of change, its potential impact, and proposed date of implementation. Usually, this form is electronic and is available on an organization's intranet. The user should provide as much detail as possible to the reviewer of the change inquiry to ensure an appropriate action can be taken.

During this stage of the process, the auditor should ensure that there is sufficient detail in the inquiry form to make a decision. Also, the auditor should check whether the business manager or someone in authority has supported the change inquiry.

Step 2: Categorization

An authorized person, usually a change manager, reviews the change inquiry and allocates a unique number that designates it as a change request. This change request number enables tracking of a specific request at any time and at any stage of the process. In many organizations a forum of senior business users meets regularly to review submitted change requests. A change management forum's decision about a change request may fall into one of three categories:

- *Accepted.* The change request has some business benefit, and it is worthwhile for further investigation or work to be undertaken.
- *Rejected.* There is no business benefit and the change request is declined.
- *On hold/further work is needed.* The forum requires further information to make a decision.

Based on the change requests that have been accepted, a further categorization based on a risk assessment needs to be undertaken by the change manager and endorsed by the forum:

- *Type A.* Change impacts multiple systems and has a customer impact. There is high technical complexity.
- *Type B.* Change impacts one system and has a customer/business impact. There is a medium level of complexity.
- *Type C.* Change impacts one system and there is a low level of complexity.

The auditor should ensure that all change inquiries have been assigned a unique number. Further, auditors should ascertain whether all change requests have been considered by the change management forum and whether the change manager has conducted a risk assessment. The auditor also should assess whether the forum's membership is appropriate and its roles and responsibilities are documented in a charter.

Step 3: Release Decision
Once a change request has been worked on and tested, it must be presented to the change management forum to ascertain whether the change can be released into the production environment. This release decision should be based on the risk assessment decision made in step 2. Before approving the release of a change, the change management forum should consider whether:

- All testing is complete and authorized by the appropriate parties. This should include user acceptance testing at a minimum, as well as stress and volume, regression, performance, and security vulnerability testing, if applicable.
- A run sheet containing roll-back and back-out procedures has been documented.
- All quality measures have been met. This is usually defined as part of the system development life cycle and is out of scope for the change management process.
- Outage impacts have been determined. This is the amount of time a system will not be available while the change is being implemented.
- Impacted business units/stakeholders have been informed that the system may not be available for a specified time period. Communication to users is only needed when there is a direct impact to them.
- System documentation has been updated.
- Operational teams are ready to support the change.

The auditor should ensure that all change requests are approved by the forum and all documentation is in place to support the decision.

Step 4: Migration
It is important that the actual migration of the change is completed by a person who is independent from the development team because there is a risk that unauthorized changes may be made to production code. In most organizations, the change manager performs this function.

The auditor should ensure that only authorized personnel can migrate code into the production environment by checking the security access profiles of users. While conducting this work, there also is some merit in checking the access profiles of developers to ensure that their access is restricted to development environments.

Step 5: Emergency Changes
At times, urgent emergency changes may be needed with no time to follow the standard process. To prepare for this scenario, the organization should develop an emergency change

management process, preferably with authorization from a senior manager or a subgroup of the change management forum. Emergency access also should be authorized by the manager or subgroup. Once the change is implemented, the key participants in the change should conduct a post-implementation review (PIR) to ascertain the impact of the change to the process and system and report the findings to the forum. A PIR also may be conducted for key changes.

From an internal audit perspective, hastily implemented emergency changes pose a great risk to the organization because they do not apply the same level of rigor and due process established for the change management process. The auditor should ensure that temporary access provided to personnel is removed promptly.

Step 6: Reporting and Tracking

All change inquiries and requests should be reported to senior management on a regular basis. An automated change management system can track and report on each unique change request number at any point in time.

The auditor should ensure that timely reports are produced and used by management. Furthermore, the auditor should ascertain that open changes are managed and closed out promptly.

MANAGING THE RISKS OF CHANGE

By following each of the steps in the change management process, organizations can manage the significant risk associated with introducing system changes. Auditors can assist their organization by ensuring that processes are in place to identify and manage these risks timely.

To comment on this article, email the author at shannon.buckley@theiia.org.