Auditing IT Risk Associated With Change Management and Application Development

Using a risk-based approach (RBA) to the IT audit begins with the IT auditor assessing the inherent risk (IR) of the relevant technologies. Some IT risks are generally high, maybe very high, regardless of the industry, type of organization or nature of the individual entity. Some examples of those risks are data transferring between information systems, using a spreadsheet for critical applications and performing customized application development in-house. This article focuses on the last item: change management for custom application development (AppDev).

The next step by the IT auditor is to investigate the control environment to see if the entity has mitigating controls for change management associated with AppDev. The IT auditor needs to assess the control risk (CR) to assess an overall risk associated with AppDev and the audit/review being undertaken. COBIT and other ISACA tools contain a rich set of knowledge and techniques related to this important risk.

This article provides the IT auditor with concepts, techniques, processes and structures that can mitigate the change management risk associated with AppDev. It also provides questions and possible sources of evidence regarding the assurance that mitigating controls could provide.

COBIT A16 MANAGE CHANGE
The COBIT 4.1 process associated with AppDev risk is A16 Manage change. This process is described as follows:

All changes, including emergency maintenance and patches, relating to infrastructure and applications within the production environment are formally managed in a controlled manner. Changes are logged, assessed and authorized prior to implementation and reviewed against planned outcomes following the implementation. This process assures mitigation of the risks of negatively impacting the stability or integrity of the production environment.

In COBIT, the control objectives related to the Manage change process are:

- A16.1 Change standards and procedures
- A16.2 Impact assessment, prioritization and authorization
- A16.3 Emergency changes
- A16.4 Change status tracking and reporting
- A16.5 Change closure and documentation

These control objectives can be achieved through various practices depending on the capability of the enterprise and the technology involved. One possible set of such practices for A16 is documented in the COBIT® Control Practices publication. The IT Assurance Guide: Using COBIT® provides auditors with guidance on how to assess the adequacy of their enterprises’ design and implementation of their change management processes, based on the COBIT control objective/control practice content.

Control over the change management process is measured by metrics such as:

- Number of disruptions or data errors caused by inaccurate specifications or incomplete impact assessment
- Amount of application of infrastructure rework caused by inadequate change specifications
- Percent of changes that follow formal change control processes

Other metrics are suggested for consideration in the COBIT A16 process content.

The benefits of the COBIT control objectives, control practices, assurance guidance and related metrics examples are that they provide the IT auditor with guidance on appropriate questions to ask in relation to change management processes and activities, suggested sources of evidence of control activities and risk mitigation, and audit procedures to perform.

For instance, in regard to AppDev, is the application programming change:
• Authorized?
  – For example, the programming change is authorized by a
    sponsor who is a business unit manager. That is, there is a
    signed and completed change management request along
    with an official business case.
  – Another example is that an approval document is
    signed by the IT steering committee or an alternate
    authorized body.
• Subjected to a risk-impact assessment?
  – If so, there should be documentation of that assessment.
    Also, a formal structure such as a steering committee
    could have this step as a standard process for all changes.
  – It is critical that all applications be assessed for impact due
    to the high nature of IR.
  – Has the risk of errors been properly assessed?
    Programming errors are probably the primary or most
    common IT risk in AppDev.
  – If a significant business application is involved, and a
    large number of lines of code are being changed, deleted
    or added, the change is, by nature, high-risk. Has the
    entity properly assessed this IR, and provided an
    appropriate mitigation?
• Handled effectively and formally when it is an
  emergency change?
  – Some emergencies require the change to be made first, and
    then the documentation and structured, formal processes
    completed, for the most part, after the emergency has been
    addressed.
  – There should be some documented definition of
    “emergency,” and documented processes for handling
    emergency changes.
• Prioritized among other IT changes in a manner that is
  effective for the entity as a whole?
  – Many times, the prioritization of IT changes defaults
    to the IT department, probably its director or the chief
    information officer (CIO). This situation is not the
    one preferred, nor the one suggested by COBIT
    (see PO4.5 IT steering committee).
  – Look for a formal structure that makes these decisions.
  – Look for a direct and interactive link between prioritizing
    major IT changes and the board of directors (BoD)/executive
    level of management (i.e., good IT governance).
• Tracked by a formal process?
  – The status of all AppDev changes is updated in a timely
    and consistent manner.

Enjoying this article?

• Read Change Management Audit/Assurance Program.
  http://www.isaca.org/bookstore
• Read Systems Development and Project Management Audit/Assurance Program.
  http://www.isaca.org/bookstore
• Learn more and collaborate on Change Management and COBIT in the Knowledge Center.
  http://www.isaca.org/knowledgecenter

  – Tracking should be a formal process, such as an
    application that requires entry of an AppDev change,
    authorization of that change before work begins, and
    testing documentation.
  – Change-related problems are identified and handled in
    a timely and proper manner by the tracking system, or
    reported to the appropriate committee, or both.
  – Reporting on AppDev progress and changes in status
    is done in a formal, structured format with regular
    consistency, e.g., reporting to a project management
    office (PMO) or change management committee
    (see following discussion).

The IT auditor needs procedures to address these questions
and the COBIT-related content referenced previously supports
this need. One audit procedure is to pull a sample of AppDev
projects for the period under review to see if evidence exists
(via inspection or observation) to obtain some assurance that
the entity has mitigated the high IR of AppDev by establishing
effective control of the enterprise’s change management
process by achieving the control objectives described in
COBIT AI6.

As a specific focus, the IT auditor should examine
enterprise documentation for evidence of the employment
of best practices of systems development life cycle (SDLC),
which are generally considered mitigating controls for
AppDev risks.4
The maturity model for AI6 described in COBIT provides a scale and supporting attributes by which the IT auditor could assess the maturity of an enterprise’s change management process.

In the process of completing the IT audit for AppDev, the IT auditor should remember that change management is enabled by an organizational structure with roles and responsibilities as well as by a process and metrics (measurements). COBIT AI6 acknowledges this multifaceted aspect by supporting process control objectives and performance measurement aspects. The structure aspect specifically related to change management activities is dealt with by the responsible, accountable, consulted and informed (RACI) chart related to AI6. The RACI chart provides guidance on change management roles and responsibilities related to generic change management process activities that support the broader organizational structure considerations addressed by COBIT in another process—PO4.

COBIT PO4 DEFINE THE IT PROCESSES, ORGANIZATION AND RELATIONSHIPS

Another way the entity can mitigate AppDev risks is to have a formal structure to deal with some of the previously mentioned responsibilities and accountabilities that enable process activities to occur in a controlled manner (e.g., authorization, prioritization, alignment with business strategy, entity to whom reports are made).

A Steering Committee

COBIT process PO4 Define the IT processes, organization and relationships applies to AppDev controls by providing a necessary formal structure. As part of COBIT’s Plan and Organize (PO) domain, this process is necessarily about the entity as a whole and the general (management) controls over IT.

PO4.3 provides one of the formal structures that is beneficial to mitigating AppDev risks. According to COBIT 4.1, PO4.3 establishes an IT steering committee (or equivalent) composed of executives, business managers and IT management (i.e., it is cross-functional). Its purpose is to:

- Prioritize IT investments and projects and align them with the enterprise’s business strategy and priorities
- Track the status of projects and resolve resource conflicts
- Monitor service levels and service improvements

Other PO4 control objectives such as PO4.5 (IT organizational structure) and PO4.6 (Establishment of roles and responsibilities) should also be taken into consideration.

As can be seen, these purposes fit the risks and needs to direct and control AppDev. Thus, the IT auditor may want to gather information and evidence about the existence of a steering committee and its operating effectiveness.

An Ideal Structure

Because a steering committee is strategic in nature, and because reporting and tracking of AppDev changes is tactical in nature (i.e., lots of things happen in a week’s time and problems need relatively immediate attention), there is a need to consider another level of structure for change control. An ideal structure would be for the BoD to establish a steering committee (or its equivalent) as a cross-functional group responsible for IT projects at the strategic level. This body would, for instance, be responsible for prioritizing and funding IT projects.

But the tactical aspects of AppDev (and other similar IT changes) are probably better suited to a tactical committee that meets more often (probably weekly, but not less than monthly) and is dedicated to solving problems and managing the IT changes hands-on. It may be appropriate for the enterprise to consider using a change management committee to oversee IT-related changes (not just AppDev) from the tactical perspective. The committee should be made up of the business sponsors, representatives of the user groups and the IT function. Tracking the status of changes and resolving conflicts might be better suited at the tactical level than the strategic level (steering committee).

A side benefit of such an organizational approach is that business-unit managers have the opportunity to see changes initiated in other units that have consequences—maybe unintentional—that affect their unit. The change management committee provides the opportunity to vet changes across the business units before certain problems occur.

This proposal is consistent with some other principles and bodies of knowledge in the IT profession. For example, a PMO performs this type of service, function and oversight for IT projects. In Capability Maturity Model Integration (CMMI) from the Software Engineering Institute, there is a hierarchy structure for software development that includes the strategic level (BoD), the middle management level (tactical) and the ground level, where programmers work. So, the change management committee idea could be integrated with a PMO or CMMI-based structure.
CONCLUSION

AppDev is an area of IT that generally is considered to be high in IR because of the probability of errors or fraud in programs when written and deployed. There need to be some reasonable mitigating controls to provide assurance that changes made to business applications do not adversely impact achievement of business objectives. The COBIT processes AI6 and PO4, and supporting materials, provide specific guidance and information to the IT auditor that can be used to gather evidence and make an assessment about the effectiveness of controls in place.

But beyond just ensuring the adequacy of the process controls that are being, and have been, employed, the auditor should also consider the adequacy of the process and organization to support the business objectives. COBIT materials support such an assessment through the guidance offered in relation to process activities, roles and responsibilities, goals and metrics, maturity levels, control practices and assurance testing.

ENDNOTES

1 IT Governance Institute, COBIT 4.1, USA, 2007
2 IT Governance Institute, COBIT Control Practices: Guidance to Achieve Control Objective for Successful IT Governance, 2nd Edition, USA, 2007
3 IT Governance Institute, IT Assurance Guide: Using COBIT, USA, 2007