Risk Assessment Management Using COBIT 5

By Vince Londini, CSPO

As a regional US grocery chain based in a major metropolitan area, FamilyGrocer (name changed) had experienced rapid growth through new store openings and acquisitions. With a focus on supply-chain efficiencies, FamilyGrocer distributes most products to its stores through a warehouse facility that also houses key offices and IT resources. In light of the risk associated with such a consolidated operation, the IT organization received a mandate from its board of directors to formally manage IT-related risk. The mandate specifically called for an initial high-level assessment of IT organizational risk, drawing largely from internal expertise. The board also requested that the IT organization demonstrate an ongoing program to manage risk.

The IT organization enjoyed a membership with Info-Tech Research group to access its best-practices research and vendor-selection guidance. Engaging with Info-Tech to conduct a COBIT-based operations workshop on risk management was a natural next step.

Info-Tech based the workshop on COBIT® 5 because of COBIT 5’s clear and concise framework for capturing key IT processes (along with process interplay and documentation requirements). COBIT is a trusted framework used by IT auditors and other IT professionals, particularly in the strategy, security and risk areas of practice.

Throughout the week-long workshop, key members of the IT management team, as well as the chief information officer (CIO), worked with the facilitator to document their insights and understanding, using COBIT to draw out their knowledge of IT risk and arrange it in a manner suitable for analysis.

The IT organization identified that it had no functioning IT risk management processes in place and, thus, assigned level zero to its process capability. The team set a goal to achieve level two (managed process) capability with performance and work-product management attributes achieved. The IT organization leveraged the Info-Tech facilitator and methodology to conduct high-level team brainstorming with key team members, aimed at identifying IT risk factors relevant to the client organization.

The team then dug in to brainstorm and document risk events, identifying actors and threat type. A prioritization rubric was developed and applied to sort the risk events. The team documented (where programs were in progress) or identified (net-new programs) the resources/time needed to mitigate the priority risk factors.

Finally, the team made critical decisions to determine the shape of the IT organization’s ongoing risk management. These included definitions of roles and responsibilities, management activities, information-gathering activities, and communication plans.

As the decisions were achieved, each was codified in the relevant program manuals, standard operating procedures, assessment tools, project requests, and templates for policies and communication.

The key outputs from this workshop included:

1. **A catalog of IT risk events**—As described previously, this catalog not only documented risk events but also the high-level mitigation strategies, initiating IT project requests as needed for items not already on their project calendar.
2. **An IT risk management program guide**—This document captured critical decisions, including the team’s rubrics for
assessing risk event severity and risk event likelihood. The document described the ongoing IT risk management steering committee process to which the team committed during the workshop.

3. **A presentation to the firm’s board on the IT risk management assessment and program**—This presentation described the progress made during the workshop, highlighted key risk factors and remediation, requested additional budget, and summarized the ongoing risk management program to the board.

FamilyGrocer emerged from the workshop with all of the process documentation required to begin executing the process the following Monday, along with the relevant to-do items needed to mitigate the identified technology, people and process gaps. The following week, the CIO presented the workshop summary to the board, which noted the thoroughness of the initial IT risk assessment and the ongoing risk management program that was designed during the workshop. Two months later, progress toward risk remediation remains strong, and IT leaders remain committed to the ongoing risk management program.

**Vince Londini, CSPO**
Serves as practice leader with Info-Tech Research Group. His recent work includes applying Info-Tech’s COBIT-based workshop methodologies to help clients in the US and Canada improve their IT risk management, project portfolio management, change management and service desk processes.

©2013 ISACA. All rights reserved.