IS audit basics

Challenges Addressed by Fundamentals

Challenges set before auditors today are imposing. With seemingly endless changes in technology and the resulting effect on organizations, there is a tendency to feel overwhelmed. There might be a sense of urgency to rush audit resources to new risk areas. In the midst of change, it is important to keep a focus on audit fundamentals: It is still management's responsibility to mitigate risk and audit's responsibility to evaluate the controls implemented by management. Managers can be helped by audits that gauge organizational elements that should be in place to enable management to fulfill its responsibility.

Probably the most fundamental type of audit within an auditor's charge is a general controls review. The importance of general controls should not be underestimated. Performing reviews of specific technologies is important, but optimizing an organization's control structure is essential to its success. General controls are as important to an organization as blocking and tackling are to an American football team. Can you imagine a coach telling his team, "We have that blocking and tackling thing down so we are going to spend the rest of the year working on trick plays"? The coach would likely come to regret such an approach.

IT auditors with decades of experience who have written, read and reviewed hundreds of audit findings have observed that it is rare for a finding in an audit report to be the result of one person making an error. People make mistakes, but effective processes include controls to minimize errors. Processes should contain basic control activities such as approvals, reconciliations and monitoring. This is also true of the enterprise as a whole: Proper balances should be in place to govern the entire organizational structure.

The COBIT® 5 framework[1] provides a good basis for a review of an organization's structure through the seven categories of enablers. The central enabler is identified as "frameworks," along with related policies and principles. The goal of this primary enabler is to bring order to the management system. The framework emphasizes the interconnectedness of enablers. The goals of each enabler strengthen other enablers. The importance of seeing the full set of enablers as an interconnected system is vital to understanding the frameworks. Enablers provide a prism for evaluating the effectiveness of an organization's structure. The COBIT 5 enablers include:

- Principles, policies and frameworks
- Processes
- Organizational structures
- Culture, ethics and behavior
- Information
- Services, infrastructure and applications
- People, skills and competencies

After the primary enabler of "processes" and "organizational structures" are the next two enablers within the COBIT 5 hierarchy. These components are fundamental to the success of all other enablers. Organizational structure and processes are the basis for most general controls. A general controls audit of an organization's structure and processes provides a means to identify general problems before specific problems arise. An effective set of steps for performing a general controls review can be taken directly from COBIT 5 guidelines by using its principles to conduct the audit.

Gordon Stoor, CISA, CISSP, ISO 20000 AC, ISO 20000 LA
Is an IT auditor with more than 30 years of experience in information technology, the last 20 of those years as an IT auditor. He has performed and supervised many types of audits, including numerous audits to ensure conformance with accepted standards/frameworks including COBIT® and ISO 20000. Currently, he works for the Florida Agency for Health Care Administration as an IT auditor.

There is conformance in the principles found within various service-oriented frameworks accepted within the industry. Frameworks such as COBIT 5 and ISO/IEC 20000[2] contain specific guidance for the governance and management of IT services. The guidance within these frameworks and standards includes a comprehensive set of best practices for information service processes. These directives provide valuable criteria for performing IT audits. COBIT 5 and ISO/IEC 20000 specifically name process functions that should be a part of IT service management. While there are minor differences in the way the two frameworks organize the processes, there is consensus regarding the operational processes that should be present. A consolidated list of these processes follows:

- Project management
- Service-level management
- Service continuity and availability management
- Budgeting and accounting
- Capacity management
- Information security
- Relationship management
- Supplier management
- Service request and incidents management
- Problem management
- Configuration management
- Change management
- Release and deployment management

The concept of general controls involves elements such as completeness, validity, identification, approvals, reconciliations, inventory and monitoring. Each of these 13 processes emphasizes at least one of these control elements for the benefit of the organization. Like COBIT 5 enablers, the operation of these processes is interrelated, and together they help ensure that the IT section effectively supports the needs of the organization as a whole. There are many dependencies among processes, so if one process is deficient, other processes are affected.

This consolidated list can provide a starting point for a general controls review of organizational structure and processes. The first step in this review would involve a top-down examination of the organization to identify that these service processes are in place. Any of the processes not in place would be an exception and would probably be considered a deficiency. Each process does not need to have a dedicated organizational unit, but as a best practice, all services should be identifiable within the organization.

“There are many dependencies among processes, so if one process is deficient, other processes are affected.”

The frameworks contain many best practices specific to each process; however, for the purposes of a general controls review, criteria can be limited to basic process principles. By definition, a process has inputs, activities that add value and outputs. A process is never stand-alone because this would serve no purpose. COBIT 5 includes a Process Model[3] that describes high-level principles necessary for a process to be effective. These principles include documented stakeholders, assignment of responsibility, defined goals, defined process activities and monitoring. These principles can serve as review criteria for examining separate processes.

After the processes are identified, their conformance with accepted principles can be analyzed. Each process should have a process manager who has been assigned responsibility for the process. An examination of organizational charts and position descriptions are a useful part of this review, but interviews are also necessary.

Interviews help determine whether accountable individuals understand and accept their roles and responsibilities. Each process will have at least one other process that depends on its output. From a process perspective, the managers who rely on these outputs are stakeholders. Since these stakeholders benefit from process outputs, they should have insight into the effectiveness of the processes on which they depend. Process managers should be interviewed regarding their direct knowledge of other processes as well as their own process. This step should provide the auditor with insight and possibly findings regarding the organizational structure.

The importance of written policies and procedures should not be understated. This is where the activities that carry out the process are documented. A review of related policies and procedures will provide an understanding of the level of planning and direction managers have dedicated to the process. Written procedures demonstrate management's efforts to organize the activities of a process. The review of written procedures is a key step in a general controls review because the auditor will be identifying specific controls within each process. Control elements such as approvals and monitoring should be assessed for reasonableness. The presence of minimal written procedures should result in a finding.

> **"Audit results are only as good as the criteria used for the evaluation."**

In a general controls review, the auditor focuses on activities that provide assurance that the process is effective. The importance of different control elements varies between processes. It is clear that the change management process would need well-defined completeness and approval controls, while configuration management should have strong inventory-related controls. The internal controls within service processes are the simple activities that help assure that the goals of the process are met. The internal control should be a defined activity having some recognizable benefit. Selecting control activity results to review will provide assurance of a control's effectiveness. Not all controls can be tested, but if the controls are well defined and responsible, workers understand their task and some assurance can be gained.

The principle that processes have defined goals is important to consider throughout the review. The acceptable level of process output quality or quantity affects how strictly internal controls are enforced. A higher level of quality will require a stricter enforcement of internal controls. Internal control activities should be evaluated in terms of the goals of the process. Process monitoring is dependent on defined goals in order to manage effectively. For larger processes, effective monitoring is almost impossible without some performance measurement data. Process reports should contain information relating to the achievement of its goals. The auditor would probably record a deficiency if a process does not have a means for gauging its success. The ISACA® publication *COBIT 5: Enabling Processes*[4] provides multiple process measures that can serve as report recommendations for processes needing measurements.

Conclusion

Audit results are only as good as the criteria used for the evaluation. A general controls audit of an IT organization based on organizational structure and process best practices should provide management with specific recommendations for improvement. The best practices criteria found in the COBIT 5 and ISO/IEC 20000 frameworks provide authoritative support for audit recommendations. The review may also highlight areas that should be examined at a more detailed level later. The more detailed review would utilize the specific principles found in the frameworks for process criteria. In a time of constant change, audit fundamentals should not be ignored.

Endnotes

1 ISACA, COBIT 5, USA, 2012, *www.isaca.org/COBIT/Pages/default.aspx*
2 International Organization for Standardization, ISO 20000, *Information technology—Service management—Part 1: Service management system requirements*, *www.iso.org/iso/catalogue_detail?csnumber=51986*
3 *Op cit,* COBIT 5
4 ISACA, *COBIT® 5: Enabling Processes,* USA, 2012, *www.isaca.org/COBIT/Pages/COBIT-5-Enabling-Processes-product-page.aspx*