CHAPTER SEVEN

Infrastructure Controls and ITIL Service Management Best Practices

CHAPTER 6 DISCUSSED AUDIT procedures for reviews of information technology (IT) general controls; these are the persuasive types of controls that are installed throughout an enterprise's IT systems operations and provide protection for all systems and applications. Examples of general controls might be physical locks and other security controls for a hardware server center or a common IT password security system covering all enterprise IT operations. As Chapter 6 emphasized, weak IT general controls will impact all IT applications that are part of those systems operations.

In today's world of pervasive IT processes and systems, installed throughout the enterprise and ranging from an application, to control of an accounting general ledger, to the all-pervasive Internet, IT auditors should have a strong understanding of IT internal control techniques. Although the lines of separation are sometimes difficult, we generally can think of IT controls on two broad levels: application controls that cover a specific process (such as an accounts payable application to pay invoices from purchases) and general IT controls. This latter category covers many controls that go beyond those discussed in Chapter 6; they do not relate just to specific IT applications and are important for all aspects of an enterprise's IT operations.

The concept of IT general controls goes back to the early days of centralized, mainframe computers. Today we often think of the set of processes that cover all enterprise IT operations as the IT infrastructure. This IT infrastructure is very different across enterprises, large and small, due to the relative size of their operations and the overall nature of their business. Because of the many possible variations in the types and sizes of IT systems and facilities that may be needed, there is really no one single set of control procedures here. Rather, an enterprise should implement a set of best practices that will guide it to establish its own IT general controls best practices.

An important internal control concept here often goes beyond how IT applications reports and other IT outputs are delivered to business users. Every business IT function supports a wide range of IT service management processes, which include such areas as problem management (i.e., how IT resolves issues with its business users) or configuration management (i.e., how IT keeps track of installed software and equipment versions). IT service management covers a wide range of internal control issues, and there are some well-recognized best practices that an enterprise should install.

This chapter looks at IT infrastructure general controls based on the set of worldwide recognized best practices called the Information Technology Infrastructure Library (ITIL). These ITIL-recommended service management best practices outline the type of framework an internal audit should consider when reviewing IT internal control risks and recommending effective IT general controls improvements. Because there is never a single definition for what is considered best, some refer to these as just good practices. We prefer to use the term *best practices*.

ITIL SERVICE MANAGEMENT BEST PRACTICES

ITIL is an abbreviation for an actual set of technical publications, a set of best practices first developed in the 1980s by the British government's Office of Government Commerce (OGC), formerly called the Central Computer and Telecommunications Agency. It is an independent collection of best practices that was first widely recognized in IT operations first in the United Kingdom, followed by the European Union (EU), then Canada and Australia. It is now increasingly common in the United States. ITIL is a detailed framework of significant IT best practices, with comprehensive checklists, tasks, procedures, and responsibilities designed to be tailored to any IT organization. Dividing key service delivery processes between those covering IT service delivery and those for service support, ITIL has become the de facto standard for describing many fundamental processes in IT service management, such as configuration and change management.

ITIL is a formal "library" of technical publications, all published by the British OGC.[1] The publications are tightly controlled, similar to the International Standards Organization publications discussed in Chapter 18. IT auditors should be aware of ITIL and should determine if their IT functions have embraced any adopted ITIL best practices as part of their IT internal controls reviews. Our intent here is not to provide a detailed description of ITIL's service delivery components but to give internal auditors a high-level understanding of some of its components. An understanding of ITIL will allow IT auditors to better evaluate key processes and to make more effective recommendations when reviewing IT general controls.

ITIL service delivery best practices cover what is frequently called the IT infrastructure—the supporting processes that allow IT applications to function and deliver their results to systems users. All too often, IT auditors have focused their attention on the application development side of IT processes and ignored important supporting service delivery processes. An enterprise can put massive efforts, for example, in building and implementing a new budget forecasting system, but that application will be of little value unless there are good processes in place, such as problem and incident management, to allow users to report and resolve systems difficulties. Also needed are good capacity and availability processes to allow the new application to run as expected. These ITIL processes are all part of the IT infrastructure, and a well-designed and controlled application is of little value to its users without such strong service support and delivery processes in place. IT auditors should have a good understanding of these enterprise processes and then develop an appropriate test of controls. These may have been covered in an IT general controls review, but ITIL provides a good general best practices model to follow.

Although they were fairly common elsewhere in the world, ITIL best practices are now becoming widely recognized in the United States as well but have not been adequately recognized by many internal auditors. The Web site of the Information Systems Audit Control Association (ISACA) has numerous reference materials that tie ITIL best practices with the *C*ontrol *Ob*jectives for *I*nformation and related *T*echnology (CobiT) framework discussed in Chapter 2. Unfortunately, a search on the Institute of Internal Auditors' Web site at the time of this publication contains no references to ITIL. All internal auditors who perform reviews that touch IT infrastructure areas should understand internal control procedures following ITIL best practices.

The next sections provide an overview of some ITIL service delivery processes important for an IT auditor, including capacity or service-level management best practices. This should give an IT auditor some guidance on how IT functions, such as a help desk, should have effective processes in place in these very important areas of IT operations. ITIL does not specify standards for building and managing IT controls; it suggests new ways to implement and operate infrastructure general controls that should have already been in place.

ITIL service delivery strategies can be viewed as a continuous activity life cycle, sometimes shown as three embedded process activity rings. The outer ring defines continuous service improvement processes. That is, an ITIL-ready organization should have continuous service processes in place that encompass all other service management processes and receive inputs from outside IT customer sources. There are three independent, linked processes within the continuous service improvement ring—service design, transition, and operations best practices; each is discussed in later sections. In the center of these concentric rings is the service strategy process. This core process includes the IT organization policies and practices that were described in the COSO internal controls framework control environment element introduced in Chapter 1. Exhibit 7.1 shows this same service delivery model as a feedback flowchart process.

ITIL processes traditionally have been split between those covering service support and those for service delivery. Service support processes help make IT application operate in an efficient and customer-satisfying manner, while service delivery processes improve the efficiency and performance of IT infrastructure elements. There are five ITIL service support best practice processes, ranging from release management best practices, for placing an IT component into production, to incident management, for the orderly reporting of IT problems or events. ITIL service support processes cover good practices for any IT enterprise, whether a centralized operation using primarily

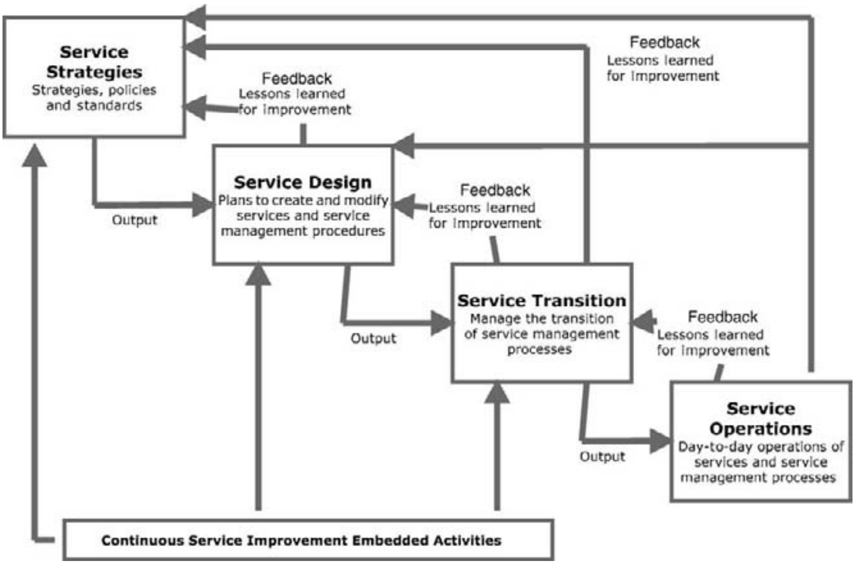
Service Strategies
Strategies, policies and standards
Feedback
Lessons learned for improvement
Feedback
Lessons learned for improvement
Output
Service Design
Plans to create and modify services and service management procedures
Feedback
Lessons learned for improvement
Output
Service Transition
Manage the transition of service management processes
Feedback
Lessons learned for improvement
Output
Service Operations
Day-to-day operations of services and service management processes
Continuous Service Improvement Embedded Activities

EXHIBIT 7.1 ITIL Continuous Feedback Loop

classic legacy mainframe systems as its IT central control point, to highly distributed client-server operations. Because of the many variations possible in an IT operations function, ITIL does not prescribe the details of ‘‘how’’ to implement service support processes, such as their configuration or change management. Rather, it suggests good practices and ways to manage inputs and relationships between these processes. There is no order or precedence among each of these best practices. They can be considered and managed separately, but all of them are somewhat linked to one another, providing a linkage between the business operations, IT technology, and infrastructure management.

Although there are many separate but interrelated elements to ITIL, we discuss only those service life cycle components that are more important for an IT auditor performing a general controls review. These ITIL best practices suggest preferred IT operations approaches to operate IT production systems in a manner that will promote efficient operations and will deliver quality services to the ultimate user or customer of these services. These best practices are particularly useful for an IT auditor performing a review and making recommendations in an IT operations area.

When IT audit is observing and reviewing IT operations internal controls, often it is useful to think of the area being reviewed in terms of the separate ITIL processes discussed in the next sections. For example, the ITIL process called incident management, or what has traditionally been called the ‘‘help desk’’ is a facility where systems users or customers call in to IT operations with a question or problem. Although a help desk function can be very useful, it is often a source of grousing when, for example, similar problems are called in repeatedly with no evident efforts to initiate a solution to the problem. Going beyond just a casual help desk and thinking of these activities as an overall process where matters are reported to other supporting processes will improve performance here and improve the overall quality of IT operations. When an IT auditor observes deviations from ITIL best practices, IT audit recommendations for performance improvement can become a major service to management.

ITIL'S SERVICE STRATEGIES COMPONENT

The upper left corner of Exhibit 7.1 of ITIL feedback loop processes shows a function called service strategies. This component describes the ITIL service management policies, strategies, and standards that provide input and direction to the other ITIL service design, transition, and operation processes. Those latter three components also provide inputs to service strategies to establish continuous process improvements.

As a best practice, ITIL suggests that an IT management team should first ask some hard questions about the quality of their IT service function, including:

- Which of our IT services or service offerings are the most distinctive?
- Which of our services are the most profitable?
- Which of our customers and stakeholders are the most satisfied?
- Which of our activities are most different and effective?

These are not the types of questions that IT management typically asks; they are seldom questions from management when assessing IT resources, and they are questions very seldom raised by IT auditors. Nevertheless, IT audit should consider these types of questions when performing a general IT controls review. The idea is to encourage the enterprise IT function to move from being from a resource that maintains IT processes and to one that provides valuable and cost-effective services to the overall enterprise. Exhibit 7.2 is a list of additional questions to help IT to improve its strategic capabilities and offerings.

- What IT services should we offer and to whom? That is, do we serve all enterprise units, a limited sample, or outside customers?
- How do we differentiate ourselves from competing alternatives? Outside service providers offer alternative services, but what are the unique costs or values that make this IT function a better alternative?
- How can we truly create value for our customers? Too often, IT handles almost redundant, required services, such as month-end financial reports that receive little attention. IT should look to see how it can better service users.
- How can we make a case for strategic investments? Rather than regularly just submitting budget requests for such matters as software upgrades, IT should carefully justify such requests.
- How should we define service quality? Through surveys and collaborative work, all interested parties should recognize how to identify quality IT services.
- How do we efficiently allocate our resources across our defined portfolio of offered services?
- How can we resolve conflicting demands for shared services?

EXHIBIT 7.2 Questions for Developing ITIL Strategic Capabilities

A multidisciplinary approach would be required for the questions in this exhibit because ITIL suggests that the IT organization should work with other functions, such as operations, finance, quality assurance, and internal audit, to better understand and define these key IT strategies for the enterprise. The whole idea is that an IT department or group should decide what it is in regard to the overall enterprise and what services it can offer. This type of introspective review may result in a service portfolio or catalog that defines IT's capabilities and service offerings.

ITIL service strategies introduce a best practices process that has been often ignored by both IT auditors and financial managers: financial management for IT services. Many IT auditors avoid this area, arguing that they are not accountants and do not need to worry about accounting-related issues. Classic financial internal auditors often see IT services as an issue that is too technical or of no interest. However, this is an important internal control area of potential concern and an ITIL best practice. Several other best practice areas under service strategies, such as organizational development, are not discussed here.

In its earlier days, the IT function in most enterprises was operated as a "free" support service with its expenses handled through central management and costs allocated to users with little attention given to IT-related costs. If a user department wanted some new application, it would pressure management to purchase the software package and add any additional necessary people to manage it. Over time, IT enterprises began to establish chargeback processes, but these were too often viewed as a series of "funny-money" transactions where no one paid too much attention to the actual costs of IT services.

Today, the costs and pricing of IT services are or should be a much more important consideration. The well-managed IT function should operate more as a business, where ITIL financial management is an important and key ITIL process to help manage the financial controls for that business. The objective of the service strategy financial management process is to suggest guidance for the cost-effective stewardship of assets and resources used in providing IT services. IT should be able to account fully for its spending on IT services and to attribute the costs of services delivered to the enterprise's customers. There are three separate subprocesses associated with ITIL financial management:

1. **IT budgeting** is the process of predicting and controlling the spending of money for IT resources. Budgeting consists of a periodic, usually annual, negotiation cycle to set overall budgets along with the ongoing day-to-day monitoring of current budgets. Budgeting ensures that there has been planning and funding for appropriate IT services and that IT operates within this budget. Other business functions will negotiate periodically with IT to establish expenditure plans and agreed investment programs; these ultimately set the budgets for IT.
2. **IT accounting** is the set of processes that enable IT to account fully for the way its money is spent by customer, service, and activity. IT functions often do not do a good job in this area. They have a wide variety of external costs, including software, equipment lease agreements, telecommunications costs, and others, but these costs often are not well managed or reported. They have enough data to pay the bills and evaluate some specific area costs, but IT functions often lack the level of detailed accounting that can be found in a large manufacturing enterprise, as an example.

The manufacturing cost accounting or activity based accounting model has applicability there.

3. **Charging** is the set of pricing and billing processes to charge customers for the services supplied. This requires sound IT accounting and needs to be done in a simple, fair, and well-controlled manner. The IT charging process sometime breaks down in an IT function because the billing reports of IT services are too complex or technical for many IT service customers to understand. IT needs to produce clear, understandable reports of the IT services used such that customers can verify details, understand enough to ask questions regarding service, and negotiate adjustments if necessary.

Financial management for IT supports the service strategy process through defined IT costing, pricing, and charging procedures. Although generally not operated as a profit center, the financial management process allows both IT and its customers to better think of IT service operations in business terms. The financial management process may allow IT and overall management to make decisions about what, if any, functions should be retained in-house or outsourced to an external provider.

The financial management process allows accurate cost-benefit analyses of the IT services provided and allows the IT enterprise to set and meet financial targets. It also provides timely reporting to the service-level management process, such that customers can understand the charging and pricing methods used. Of all of the ITIL service support and delivery processes, financial management is one ITIL best practice that frequently gets short shrift. IT people have a technical orientation and tend to think of financial management as an *accounting issue.* On the other side of the coin, finance and accounting professionals tend to look at these issues as too technical and beyond such transactions as equipment lease accounting or facility space charges. IT auditors should develop some financial skills as well as using their IT knowledge to review and assess financial management process internal controls. Exhibit 7.3 provides procedures for an internal audit review of the costs and pricing of IT processes. This is often not a common review area for internal audit, but given the large costs distributed to customers as well as the importance of an enterprise's IT resources, it can be an important audit area.

ITIL SERVICE DESIGN

ITIL service strategies support three other process areas, starting with the first phase in the service life cycle, service design. IT processes for service design cover areas more closely aligned with the smooth and efficient operation of the overall IT infrastructure. ITIL has identified five aspects of service design:

1. The design of each IT service offered, including their functional requirements, resource needs, and anticipated capabilities
2. The design of service management systems and tools, often presented through a formal portfolio, for the management and control of these services through their life cycles

1. Develop and document a general understanding of the cost structure for IT operations, including costs of equipment supplies and salaries.
2. Review and understand costing philosophy for IT operations: Is it an overhead function, cost recovery, or revenue generating?
3. Review processes for costing and pricing IT services:
   a. Are all IT costs covered?
   b. Based on interviews with IT users, does the costing and pricing system appear to be understandable?
   c. Is there a process in place to administer the costing process and to make adjustments if necessary?
4. Review the negotiation process with IT users to understand pricing process: Are expected costs included in service-level agreements (SLAs)?
5. Select pricing reports during a period for several processes and check to determine the prices are included in SLAs.
6. Review appropriateness of the adjustment process over a period of time to determine the corrections are investigated and applied when appropriate.
7. Review a sample of data processing services billed for one accounting period, and determine whether they cover all actual IT costs. Investigate and report on any differences.
8. Review the overall budgeting process for IT operations, and determine if it appears consistent with other enterprise budgeting procedures.
9. Assess whether management reviews actual IT costs and compares them to established budgets, taking appropriate remedial actions as required.
10. For a selected accounting period, trace IT pricing charges to appropriate accounting system entries.

EXHIBIT 7.3 Costs and Pricing IT Audit Review Steps

3. The design of IT architectures and management systems necessary to provide the services
4. The design of processes needed to install, operate, and improve these overall service processes
5. The design of measurement methods and metrics of the service processes and their component architectures

What this really says is that every IT function installs a lot of customer services, and these services should be managed and controlled through appropriate best practice techniques. To support efficient service delivery, ITIL has specified a series of specific processes. Some of these, such as the continuity management process, have traditionally been near and dear to the hearts of many IT auditors. Others, such as service-level agreements (SLAs) that define performance and expectations between IT and its customers should be familiar to other internal auditors who encounter similar arrangements in other areas.

Service Delivery Service Level Management

Service Level Management is the name given to the process of planning, coordinating, drafting, agreeing, monitoring, and reporting on formal agreements between both IT and the providers and recipients of IT services. This process is managed through service-level agreements (SLAs) that represent a formal agreement between IT and both providers of services to IT as well as IT end user customers. When the first ITIL service-level best practices materials were published in 1989, an SLA was an interesting but uncommon concept. Today many enterprises have introduced them—although with varying degrees of success—and IT auditors should be familiar with and understand the importance of SLAs when reviewing internal IT infrastructure controls.

As an example of an SLA, when IT contracts with an outside provider, such as for disaster recovery backups, the arrangement will be covered by a formal contract where the disaster recovery provider agrees to provide certain levels of service, following some time-response-based schedule. The governing contract here is an SLA between IT and the provider of continuity services. SLA agreements between IT and their customers are even more important, from an internal control perspective. We have used the more current term of *customer* here rather than the older and still common term *IT users*. Many groups use IT's services, and as customers, they have expectations of certain levels of service and responsiveness. These arrangements are defined through an SLA, a written agreement between the IT provider and its customers defining the key service targets and responsibilities of both parties. The emphasis should be on a mutual agreement, and SLAs should not be used as a way of holding one side or the other to ransom. A true partnership should be developed between the IT provider and the customer for mutually beneficial results; otherwise, the SLA could quickly fall into disrepute, and a culture of blame may prevent any true service quality improvements from taking place.

In an SLA, IT promises to deliver services per an agreed-on set of schedules and understands there will be penalties if service standards are not met. The goal here is to maintain and improve on service quality through a constant cycle of agreeing, monitoring, reporting, and improving the current levels of IT service. SLAs should be strategically focused on the business and on maintaining the alignment between the business and IT.

Exhibit 7.4 outlines the contents of a typical SLA. This type of document would not be found as part of a mortgage document signed at a house closing. Rather, the IT customers negotiate the IT service requirements that they are seeking, such as "average response times no more than . . ." or "financial systems close processing completed by . . ." or other factors. To temper expectations and show what could be available, an IT function usually provides a service offerings catalog. Customer IT service requirements should be negotiated and formal SLAs established. Performance against these SLAs should be monitored on an ongoing basis with performance reported regularly. Failure to meet these SLA standards could result in additional negotiations and SLA adjustments. This SLA process provides benefits for the business and IT, including:

- Because IT should be working to meet negotiated standards, IT services will tend to be of a higher quality, causing fewer interruptions. The productivity of the IT customers should improve as well.
- IT staff resources will tend to be used more efficiently when IT provides services that better meet customer expectations.
- By using SLAs, the services provided can be measured and the perception of IT operations generally will improve.

While there is no one form or format for an SLA, the following are contents that should be considered for most SLAs:

Agreement Introduction Pages

- Parties to this agreement
- Title and brief description of the agreement
- Signatories
- Dates: start, end, review
- Scope of the agreement; what is covered and what is excluded
- Responsibilities of both the service provider and the customer
- Description of the services covered

Service Hours

- Hours that each service is normally required (e.g. 24 × 7, Monday to Friday 08:00–18:00)
- Arrangements for requesting service extensions, including required notice periods (e.g., request must be made to the service desk by 12 noon for an evening extension, by 12 noon on Thursday for a weekend extension)
- Special hours allowances (e.g., public holidays)
- Service calendar

Availability

- Availability targets within agreed hours, normally expressed as percentages. The measurement period and method should be stipulated and may be expressed for the overall service, underpinning services, and critical components or all three. Since it is difficult to relate to simplistic percentage, availability can be measured in terms of the customer's inability to carry out its business activities

Reliability

- Usually expressed as the number of service breaks, or the mean time between failures (MTBF) or mean time between system incidents (MTBSI)

Support

- Support hours (where these are not the same as service hours) including arrangements for requesting support extensions
- Required notice periods (e.g., request must be made to the service desk by 12 noon for an evening extension)
- Special hours allowances (e.g., public holidays)
- Target time to respond to incidents, either physically or by other method (e.g., telephone contact, e-mail)
- Target time to resolve incidents, within each incident priority—targets vary depending on incident priorities

Throughput

- Indication of likely traffic volumes and throughput activity (e.g., number of transactions to be processed, number of concurrent users, amount of data to be transmitted over the network)

Transaction Response Times

- Target times for average or maximum workstation response times (sometimes expressed as a percentage: for example, 95% within 2 seconds)

Batch Turnaround Times

- Times for delivery of input, and the time and place for delivery of output

Changes

- Targets for approving, handling, and implementing requests for changes (RFCs), usually based on the category or urgency/priority of the change

EXHIBIT 7.4 Sample IT Service-Level Agreement Contents

IT Service Continuity and Security

- Brief mention of IT service continuity plans and how to invoke them, and coverage of any security issues, particularly any responsibilities of the customer (e.g., backup of free-standing PCs, password changes)
- Details of any diminished or amended service targets should a disaster situation occur (if no separate SLA exists for such a situation)

Charging

- Details of the charging formula and periods (if charges are being made). If the SLA covers an outsourcing relationship, charges should be detailed in an annex as they are often covered by commercial in confidence provisions

Service Reporting and Reviewing

- The content, frequency, and distribution of service reports, and the frequency of service review meetings

Performance Incentives/Penalties

- Details of any agreement regarding financial incentives or penalties based on performance against service levels. These are more likely to be included if the services are being provided by a third-party organization. It should be noted that penalty clauses can create their own difficulties

EXHIBIT 7.4 *(Continued)*

- Services provided by the third parties are more manageable when underpinning contracts are in place, and any possibilities of negative influence on the IT service provided is reduced.
- Monitoring overall IT services under SLAs makes it possible to identify weak spots that can be improved.

The SLA process is an important component of IT operations. If an enterprise IT function does not use formal SLAs, IT auditors reviewing both IT operations general controls and business services applications should consider recommending the establishment of such formal SLA processes. SLAs can create a totally new environment within IT, where all parties will better understand their responsibilities and service obligations with the SLA as a basis for resolving many issues. IT audit can use the status of an enterprise's SLAs while assessing internal controls in a variety of areas and for making strong controls improvement recommendations.

Service Delivery Capacity Management

ITIL capacity management ensures that the capacity of the IT infrastructure is aligned to business needs to maintain the required level of service delivery at an acceptable cost through appropriate levels of capacity. Through gathering business and technical capacity data, this process should result in a capacity plan to deliver cost-justified IT capacity requirements for the enterprise. In addition to a prime objective of understanding an enterprise's IT capacity requirements and to deliver against them, capacity management is responsible for assessing the potential advantages new technologies could have for the enterprise.

The capacity management process generally is considered in terms of three subprocesses: business, service, and resource capacity management. Business capacity management is the long-term process to ensure that the future business requirements are taken into consideration and then planned and implemented as necessary. Service capacity management is responsible for ensuring that the performance of all current IT services fall within the parameters defined in existing SLAs. Finally, resource capacity management has more of a technical focus and is responsible for the management of the individual components within the IT infrastructure. The multiple inputs to these three capacity management subprocesses include:

- SLAs and SLA breaches
- Business plans and strategies
- Operational schedules as well as schedule changes
- Application development issues
- Technology constraints and acquisitions
- Incidents and problems
- Budgets and financial plans

As a result of these multiple inputs, the capacity management process—often under a single designated capacity manager—will manage IT processes, develop and maintain a formal capacity plan, and ensure certain capacity records are up to date. In addition, the capacity manager must be involved in evaluating all changes to establish their effect on capacity and performance. This capacity evaluation should happen both when changes are proposed and after they are implemented. Capacity management must pay particular attention to the cumulative effect of changes over a period of time that may cause degraded response times, file storage problems, and excess demand for processing capacity. Other capacity management process responsibilities include some duties of the network manager and the application and system manager. They are responsible for translating the business requirements into the required capacity to meet these requirements and to optimize IT performance.

Smaller enterprises and many IT facilities, of course, may not be able to justify a full- or even a part-time capacity manager. However, some resource within the IT organization should have responsibility for capacity management issues. It is an important service design issue.

The implementation of an effective capacity management process offers IT the benefits of an actual overview of the current capacity in place and the ability to plan capacity in advance. Effective capacity management should be able to estimate the impact of new applications or modifications as well as provide cost savings that are in tune with enterprise operations requirements. Proper capacity planning can significantly reduce the overall cost of ownership of an IT system. Although formal capacity planning takes time, internal and external staff resources, and software and hardware tools, the potential losses incurred without capacity planning can be significant. Lost productivity of end users in critical business functions, overpaying for network equipment or services, and the costs of upgrading systems already in production can more than justify the cost of capacity planning. This is an important ITIL process, and IT auditors should consider the capacity management processes in place when reviewing IT infrastructure general controls.

Service Delivery Availability Management

Enterprises today are increasingly dependent on their IT services being available 24 hours a day and 7 days per week (24 × 7). In many cases, when those IT services are unavailable, the business stops as well. It is therefore vital that an IT function manage and control the availability of its services. This can be accomplished by defining the requirements from the business regarding the availability of the IT services and then matching them with the possibilities of the IT enterprise.

Availability management depends on multiple inputs, including requirements regarding the availability of the business; information on reliability, maintainability, recoverability, and serviceability; as well as information from the other processes, incidents, problems, and achieved service levels. The objectives of the availability management process are to:

- Produce and maintain an appropriate and up-to-date availability plan that reflects the current and future needs of the enterprise.
- Provide service and guidance to all other areas of the enterprise on IT availability-related issues.
- Ensure that service availability achievements meet or exceed targets, by managing service and resource-related availability performance.
- Assist with the diagnosis and resolution of availability-related incidents and problems.
- Assess the impact of all changes on the availability plan and the performance and capacity and capacity of all services and resources.
- Ensure that proactive measures are implemented wherever those actions are cost justifiable.

Availability management activities can be described as planning, improving, and measuring actions. Planning involves determining the availability requirements to find out if and how IT can meet them. The service-level management process, discussed previously, maintains contact with the business and will be able to provide appropriate expectations to availability management. Businesses may have unrealistic expectations regarding IT systems availability when they do not understand what systems availability means in real terms. For example, business users may want 99.9% availability yet not realize that this will cost five times more than providing only 98% availability. It is the responsibility of service-level management and the availability management process to manage such expectations.

Exhibit 7.5 shows this availability and costs relationship. It does not cost very much to keep basic IT systems running, but that is all the enterprise will receive. Both management and IT auditors should keep this relationship in mind when reviewing controls and making recommendations.

An IT function can design for either "availability" or "recovery." When the business cannot afford a particular service downtime for any length of time, IT will need to build resilience into the infrastructure and ensure that preventive maintenance can be performed to keep services in operation. In many cases, building "extra availability" into the infrastructure is an expensive task that can be justified by business

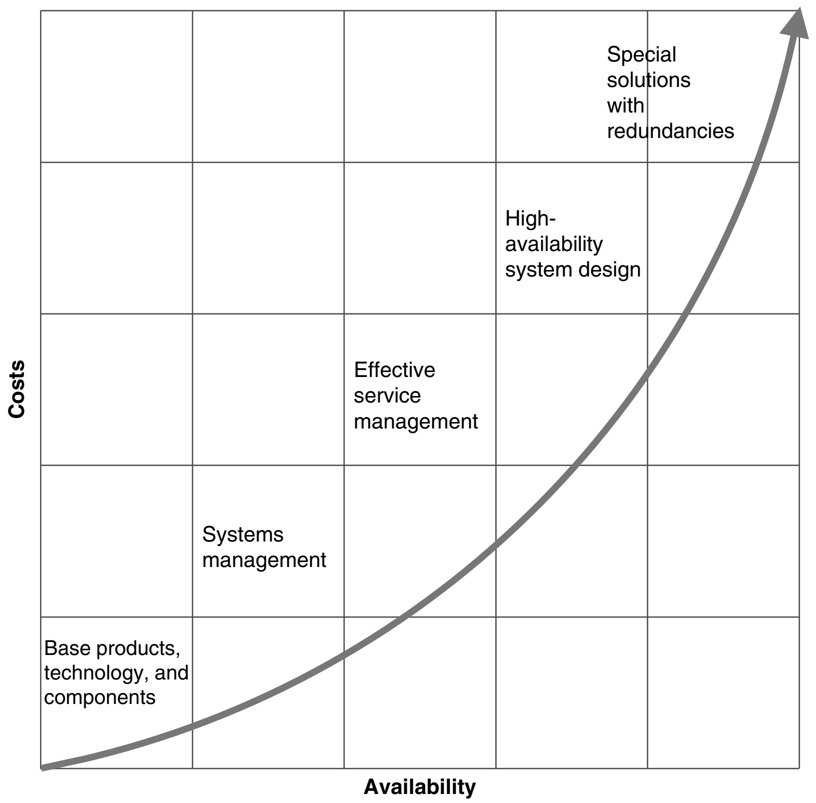

EXHIBIT 7.5 IT Availability and Cost Relationships

needs. Designing for availability is a proactive approach to avoiding downtime in IT services.

When the business can tolerate some downtime of services or when a cost justification cannot be made for building in additional resilience into the infrastructure, designing for recovery is the appropriate approach. Here, the infrastructure will be designed such that in the event of a service failure, recovery will be "as fast as possible." Designing for recovery is a more reactive management approach for availability. In any event, other processes, such as incident management, need to be in place to recover as soon as possible in case of a service interruption.

The main benefit of availability management is to have a structured process in place to deliver IT services that meet the agreed requirements of the customers. This should result in a higher availability of the IT services and increased customer satisfaction. Availability management covers an area where IT auditors often can ask some hard questions as part of their IT general controls reviews.

Service Delivery Continuity Management

As businesses are becoming ever more dependent on IT, the impact of any unavailability of IT services has increased drastically. Every time service availability or performance is reduced, IT customers cannot continue with their normal work. This trend toward a high dependency on IT support and services will continue and increasingly influence direct customers, managers, and decision makers. ITIL continuity management emphasizes that the impact of a total or even partial loss of the IT services should be estimated and continuity plans established to ensure that the business, and its supporting IT infrastructure, will always be able to continue.

ITIL calls for an appropriate strategy to be developed that contains an optimal balance of risk reduction and recovery options. ITIL also calls for some of the same business continuity and disaster recovery strategies as are discussed in Chapters 23 through 25 on IT disaster recovery and continuity management. Using the approaches outlined there, an IT organization can implement an effective set of service continuity processes. IT auditors should refer to those chapters to better understand and evaluate continuity and disaster recovery planning processes.

Service Delivery Information Systems Security Management

IT security management is another set of best practices, included in this book as part of Chapters 26 to 28. ITIL recognizes the need for information systems security within the corporate governance framework to provide a strategic direction for security activities and to ensure these activities are achieved. ITIL emphasizes that security is more than just an IT issue; it should be a management issue. The objectives of IT security are to protect the interests of those relying on IT information and the systems and communications that deliver it with the following ITIL information security objectives:

- **Availability objective.** Information is available and usable when required, and the systems that provide it can appropriately resist attacks and recover from or prevent failures.
- **Confidentiality objective.** Information is observed or disclosed to only those who have a right to know.
- **Integrity objective.** Information is complete, accurate, and protected against unauthorized modification.
- **Authenticity and nonrepudiation objective.** Business transactions as well as information exchanges between enterprises, or with partners, can be trusted.

ITIL information security management goes on to outline best practices for a complete information security management system. A very important best practice, information security management processes, are discussed in Chapter 19. An IT auditor should have the ability both to recognize the key elements of an effective information management system and to make recommendations to improve and enhance existing systems when appropriate.

ITIL SERVICE TRANSITION MANAGEMENT PROCESSES

As IT auditors recognize, IT operations almost always have been subject to regular hardware or software changes, These changes may involve proper transition planning