

realtimepublishers.comtm

The Practical Guidetm To

Securing Assets



Rebecca Herold

The Practical Guide to Securing Assets.....	1
Identifying Critical Infrastructure Systems and Information Assets	1
Why are Assets Important?.....	2
Consider People and Processes First.....	2
Effectively Secure IT Assets by Leveraging Business Operations Management Solutions	3
Enterprise-Wide Security	3
Understanding the Typical Friction Between IT Security and Business Operations.....	4
Addressing Security Governance and Business Operations Implementation.....	7
Improving Profitability Through People and Technology.....	9
Incorporating IT Management and Security into the Enterprise Mission, Goals, and Processes	9
Using a Shared Service Implementation Program to Protect Information and IT Assets	10
Balancing IT Security Activities with Business Assets and Operations.....	11
Securing the Complete Enterprise	13
Reporting the Big Picture.....	14
Simplify Security to the Amount Necessary to Support Business.....	14
Bringing IT Value to Business Units	15
Using Leading Practices to Simplify the Information and IT Security Process	16
BS 7799 and ISO 17799	17
COBIT.....	18
Reducing and Eliminating Unnecessary Information Collected Through Network Security Monitoring	20
Implementing Service-Driven Security Controls.....	21
Using IT Operations Frameworks for Service-Driven Controls.....	22
Considering Internationally Used IT Operations Frameworks	22
Using ITIL	24
Using the Microsoft Operations Framework	26
Comparing MOF to ITIL	27
Building an Asset Security Roadmap	28
Putting It All Together	28
Configuration Management	28
Incident and Problem Management	29
Change Management	30

Service/Help Desk	30
Release Management	31
Service Level Management.....	32
Capacity Management	33
Continuity Management, Disaster Recovery, and Business Continuity	33
Availability Management.....	35
IT Financial Management.....	36
Summary	37
Appendix A.....	38

Copyright Statement

© 2004 Realtimedpublishers.com, Inc. All rights reserved. This site contains materials that have been created, developed, or commissioned by, and published with the permission of, Realtimedpublishers.com, Inc. (the "Materials") and this site and any such Materials are protected by international copyright and trademark laws.

THE MATERIALS ARE PROVIDED "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. The Materials are subject to change without notice and do not represent a commitment on the part of Realtimedpublishers.com, Inc or its web site sponsors. In no event shall Realtimedpublishers.com, Inc. or its web site sponsors be held liable for technical or editorial errors or omissions contained in the Materials, including without limitation, for any direct, indirect, incidental, special, exemplary or consequential damages whatsoever resulting from the use of any information contained in the Materials.

The Materials (including but not limited to the text, images, audio, and/or video) may not be copied, reproduced, republished, uploaded, posted, transmitted, or distributed in any way, in whole or in part, except that one copy may be downloaded for your personal, non-commercial use on a single computer. In connection with such use, you may not modify or obscure any copyright or other proprietary notice.

The Materials may contain trademarks, services marks and logos that are the property of third parties. You are not permitted to use these trademarks, services marks or logos without prior written consent of such third parties.

Realtimedpublishers.com and the Realtimedpublishers logo are registered in the US Patent & Trademark Office. All other product or service names are the property of their respective owners.

If you have any questions about these terms, or if you would like information about licensing materials from Realtimedpublishers.com, please contact us via e-mail at info@realtimedpublishers.com.

The Practical Guide to Securing Assets


Keeping your information technology (IT) systems and information secure in the face of constant changes in hardware, software, threats, and regulations can seem like an impossible task. You must constantly monitor and evaluate asset security controls effectiveness in addition to monitoring regulatory and contractual security requirement compliance. To be effective, you must implement IT controls in context with your entire organization assets.

Consider the following:

- The number of security- and privacy-related laws and regulatory requirements is growing more quickly than ever before. Multiple countries, including the United States government at the federal and state level, have already passed several laws that impact how organizations must address security and privacy issues.
- Information security historically was treated primarily as a technology issue within most organizations. However, today, the CIO or CISO alone cannot address all information security issues and requirements; information security must be considered with a fresh perspective as part of the overall, larger business governance process.
- Organizations who have successfully implemented an information security program reveal a consensus in the need to adopt leading and best practices and incorporate them into the organization's IT and business operations framework.
- Information security progress will suffer without a governance framework that documents and instructs personnel at all levels of the organization. Without an appropriate framework, it is difficult to ensure that all aspects of security are completely and consistently addressed and integrated with the organization's business.

Identifying Critical Infrastructure Systems and Information Assets

Critical infrastructures are those systems and assets, including physical and electronic, that are so vital to your organization that if they were incapacitated or destroyed, they would have a debilitating impact upon your business. Every day thousands of unauthorized attempts are made to intrude into the computer systems of major government and industry networks—such as defense facilities, power grids, financial institutions, healthcare systems, government agencies, telephone systems, and transportation systems. Although many of these attempts fail, some gain systems administrator rights, crack passwords, plant malicious code and sniffers to copy transactions and sensitive files, or insert trapdoors to permit an easy return into the system. Organizations are vulnerable to such attacks because of how dependent virtually all are upon computer networks for many essential business services.

 Businesses have become dependent upon technology systems but most have paid little attention to protecting those networks. Water, electricity, gas, communications (voice and data), rail, aviation, financial, healthcare, manufacturing, and other critical functions are directed by computer controls over vast information systems networks.

Why are Assets Important?

The Gartner Group reported that approximately 40 percent of business applications downtime is caused by operational errors, another 40 percent is caused by application errors (most often misconfigurations), and the remaining 20 percent is caused by actual platform problems, including the network, operating system (OS), or hardware (Source: Lanowitz, Theresa; *Tearing Down the Wall*, Gartner Group, 2002). Such downtime impacts businesses more than it ever has before. Network systems components now support an extended network of customers, business partners, and related applications. IT professionals must constantly monitor and maintain systems to provide for sufficient (typically 24 × 7 continuous) availability and service levels.

The cost of human resources is also on the rise. Meta Group estimates that by 2006 and 2007, IT salaries will escalate, putting labor costs at 55 percent to 60 percent or more of the IT budget. (Source: Passori, Al, Maria Schafer; *Base Hit: IT Organization Field of Dreams*, Meta Group, 24 May 2004). IDC estimates that acquiring and maintaining one IT staff person costs between \$110,000 to \$120,000 annually in U.S. currency (Source: Michael Boyd, Ph.D., International Data Corp., in *Business Finance*, May 2000).

Increased processing complexity, the need for consistent and continuously reliable service levels, and increased labor costs all compound the need for securing assets to ensure that they are accurate, available, and confidential where necessary. Disruptions in service will result in increased costs to the customer in addition to operational deficiencies and increased costs to the business. A strong operational business framework that incorporates appropriate information and technology security is necessary for business success.


Consider People and Processes First

Integrate people and processes with the business technology to reduce costs and simplify, as much as possible, involved operational complexity. For example, when using a shared pool of IT resources to manage multiple clients, well-defined and comprehensive processes and procedures must be followed for the organization to be successful. IT management must understand and supervise the complex and multiple uses of resources by one customer to avoid impacting another. IT personnel must be able to make these operations possible while maintaining consistent and acceptable service levels for all customers.

Personnel issues are the most often overlooked component within IT operations. IT staff often use outdated or inadequate tools or procedures when managing the network and business processes. Such inadequacies put information assets at risk. There are an abundance of tools to assist IT staff with efficiently managing and successfully security information and technology assets. However, most organizations do not use good practices to link the technical processes of managing systems into the business and people issues that are involved. People and process must be built into the technology. This idea is supported by a Gartner report that stresses that network and system management (NSM) investments must manage the business “process, not the technology” (Source: *Manage the Process, Not the Technology*, Gartner Inc., September 2002).


Effectively Secure IT Assets by Leveraging Business Operations Management Solutions

Organizations can leverage a variety of service management solutions to manage the people and processes associated with problem, incident, or change management. Unfortunately, there are no such systems that provide a comprehensive solution that extends to the human and technology levels. What then results is the IT organization has little insight or control over tracking the progress of business activities, knowing whether business activities have been completed, or identifying the persons who are performing business tasks—or even if the persons performing the tasks are the appropriate ones to do so. As a result, gaps exist between service management systems and the business service delivery processes supporting the underlying operational infrastructure, creating inefficiencies of personnel and technology, and putting assets at risk.

 Utilizing the right tools will enable business leaders to more effectively identify operational problems and, as a result, more effectively protect business information and technology assets. The human and business operations elements must be effective to ensure the security of the underlying information and technology assets.

Enterprise-Wide Security

The typical organization structure virtually separates business operations from technology and related security operations. As a result, the IT organization has no insight into the business requirements or activities, and the business units have little understanding about all the activities, processes, and technologies necessary to help ensure business information asset security. Significant gaps then exist between the activities business unit leaders take to secure information and technology assets, and the activities that the IT organization has established, or believes are occurring, to sufficiently protect these assets. Such gaps leave organizations at significant risk for becoming victims of the multiple IT threats that exist in today's cyber environment, which could ultimately lead to devastating business loss or failure for the organization.

 Information security professionals must take it upon themselves to educate business unit leaders about the role security has throughout the organization. Such security education is one of the pillars of security best practices.

Understanding the Typical Friction Between IT Security and Business Operations


IT processes are comparatively new within the long, large history of business. Over the past several centuries, and even in recent decades with the implementation of more modern business operational processes, business unit leaders were accustomed to calling all the shots with regard to the products and services for which they were responsible. With the advent of widespread mainframe business processing in the 1960s, businesses realized that operations could be streamlined with technology, but the ultimate decisions for how technology was used was typically made by the business unit leaders. The IT support areas basically existed to keep the processing going from a large, centralized location within the organization.

It has only been in the last decade or two that highly distributed and widely mobile computing has been incorporated—almost accidentally or by choice without discussion within the IT area—into business unit processes. During this time, it has also been a popular trend to decentralize all business management decisions to the business unit leaders, giving them complete autonomy for how they run their own individual operations. The opinion was that the business unit leaders knew their services and products best, so they should ultimately be able to make the best decisions for how to run their operations.

As a result of this highly decentralized, autonomic method of establishing business operations, the organization's centralized IT support areas were, and are, often not included in important business discussions for new information handling and processing plans within the decentralized business operations. Unfortunately, this disjointed method of managing diverse business units has resulted in gaps that put information and technology at risk:

- Business unit leaders often do not understand the extent to which technology supports their business processing.
- IT leaders and personnel are often focused upon their narrow scope of technology responsibilities and do not understand the actual business operations that occur in the other parts of the organization. IT may be so focused on technology that they forget they exist to support the business. For example, IT may refuse to grant a reasonable, justifiable request for an exception to an IT standard, even though forcing a business unit to follow the standard will severely impact business.
- Business unit personnel typically do not have any training or awareness for how technology is incorporated into the business operations.
- IT personnel typically do not have any training or awareness for the products or services that the business units are responsible for managing to generate revenue for the company.
- Business unit goals and objectives are often created without consideration for IT goals and objectives. A business unit might forget, or not realize, what IT has to do within the infrastructure to support the business unit's request. For example, a business unit might try to create an enormous database without considering the problems of backing up or finding storage for such a large database.
- IT goals and objectives are often created without consideration for business unit goals and objectives.

-
- IT security has historically created security mandates based upon outside standards and best practices that were not aligned to the organization’s actual business operations and goals.
 - Business units have historically created goals and structured operations that did not consider or align with actual IT security capabilities. For example, business units often make promises to their customers without considering how to technically implement the promises. This scenario results in IT scrambling to support an initiative without sufficient resources, testing, training, consideration of security, and so on.
 - Business units often do not understand the limitations and complexities of technology and assume that technology can support all of their business operations successfully.
 - IT often does not understand the services and products created and supported by the business units. In addition, IT makes assumptions about the requirements for the systems and applications that businesses request and implement in ways that leave gaps in actual requirements or do not truly meet business needs.
 - There is often a lack of documented requirements and clearly defined roles and responsibilities with no clear identification of business process and information owners.
 - IT may not deliver as promised. For example, IT may not deliver the product or service the business wanted, the product or service might not be delivered on time, the development process for the product or service might go over budget, and so on. Regardless of whether this shortcoming occurs as a trend or only a single time, if the business perceives IT negatively, barriers between business and IT are created that are difficult to remove.
 - IT is perceived as adding layers of process, governance, and technical requirements that the business sees as slowing them down when they have deadlines to meet. As a result, business then may try to work around IT by hiring their own technical staff, outsourcing technical aspects of a project, or just plain ignoring the IT aspects until they get into trouble and need help.
 - Business may have the misperception that IT is “IT-centric” and does not understand business processes. As a result, they may not contact IT until they find a business process is broken or insufficient. When this happens throughout the organization, IT ends up supporting disparate and custom solutions, instead of using the more efficient holistic approach to problem solving from a technical and business process view.
 - Business units and IT may classify information assets differently because of disagreements regarding the importance of the asset. This disparity may result in friction between business units and IT. Poor criticality classification negatively affects asset protection and business continuity planning.


 Business units must own the business processes and information, and IT must enable the business to perform the processes.

Stakeholders for business operations should ask and understand the answers to important questions. Table 1 provides examples of such questions.

Stakeholder	Must Know and Understand
Executive management and Board of Directors	What value does IT provide? Does IT enable or disable business growth? Does IT advance organizational innovation? What value does IT security provide?
Business unit management and personnel	What value is obtained for IT investments? How does IT impact customer interactions? Does IT enhance productivity? Does IT position the business for future market demands?
IT security, audit, and regulatory compliance	Are the organization's assets and operations adequately protected? Are business and technology risks and threats being appropriately managed? Are all applicable regulatory requirements being addressed?
IT organization	Is the IT area doing the right things? Is IT effective? How can IT improve goals? Do IT activities and services meet stakeholder expectations and needs? How can IT keep staffed with qualified personnel?

Table 1: Example questions that business operations stakeholders must ask and understand the answers to.

IT and business units can reduce the friction that often exists by establishing an ongoing communications path to address stakeholder questions and concerns. Additionally, training and ongoing awareness of business operations and IT issues must occur to ensure that assumptions and faulty understanding do not lead to security gaps and noncompliance. To ensure business success, IT and business units must understand key investment decisions regarding IT and security, and include business in developing new applications and systems. Strategic relationships will ensure the success of both the business units and IT in obtaining value for IT investments.

 Successfully securing information and technology assets requires the elimination of friction between IT and business operations through training, awareness, ongoing communications, and the incorporation of IT into all business unit decisions and plans as well as business unit input into all major IT decisions and plans.

Addressing Security Governance and Business Operations Implementation

Organizations are starting to realize the need to implement a service delivery strategy to ensure appropriate implementation of tools and processes between business units and IT support areas. Such a strategy will close the gaps between business unit management and technical support and service delivery (see Figure 1).

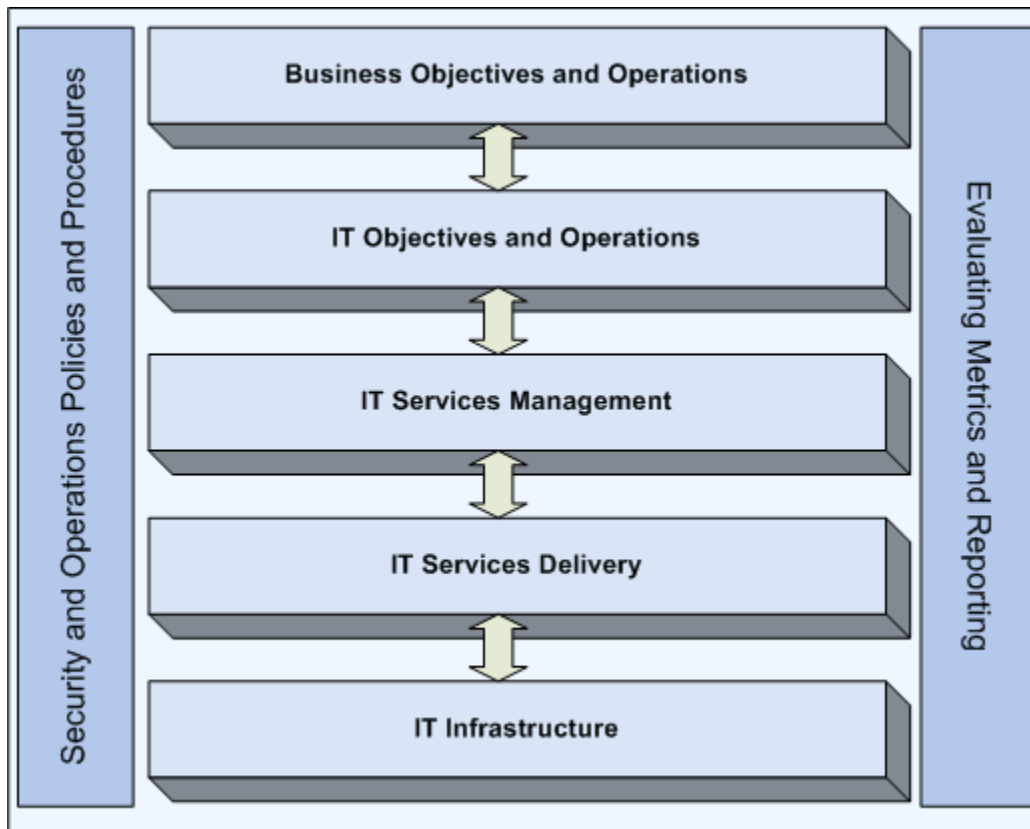



Figure 1: An IT service delivery strategy that appropriately implements tools and processes among business units and IT support areas.

Remember that business objectives must guide IT objectives and processes; IT must define and manage mutually agreed upon service levels specific to each business unit; IT service delivery must address the human side of IT by tracking, guiding, and implementing actions throughout the entire infrastructure; IT infrastructure includes all processing components, including servers, applications, databases, networks, monitoring and reporting tools.

Security professionals need to understand that security controls must help the organization to achieve an acceptable level of risk and close regulatory and contractual compliance gaps without negatively impacting business. It is not only unrealistic to attempt to achieve 100 percent security; it would be bad for business to try to do so.


Business operations must be monitored as part of security activities. An operations monitoring solution should track individual activities such as file changes, process activity and direct access. The solution should provide a consolidated view of individual activities across diverse and complex business enterprise infrastructures. Operations monitoring will allow more precise assessments of operational effectiveness and will ensure that business objectives and necessary service levels are met.

 Service delivery strategies can be integrated with service management systems to allow IT organizations to track and guide actions, from request through execution to review, completion, and evaluation.

Service delivery systems can track actual changes for comparison with approved changes. These systems can also ensure that changes occur within the bounds of established policies, including necessary approvals and procedures. Service delivery strategy goals are to more accurately verify approved changes, detect or prevent unapproved changes, and over time standardize how changes are performed. Service delivery systems should have the capability to track, enforce, validate, and report activities:

- **Track**—Service delivery systems should identify and document all change activities, including changes associated with approved change requests as well as changes made without approval. Documented changes should be available for review by authorized personnel at any time.
- **Enforce**—Service delivery systems should enforce the organization’s policies for how and when changes can be made and who can make them. For example, if a change is approved to occur within a specific time frame, the entity making the change should not be allowed to make the change outside of the indicated time frame.
- **Validate**—Service delivery systems should validate that required change processes are followed. For example, if six steps are required to delete a user account upon employee termination, the system should ensure that the six steps are completed successfully. Service delivery systems should also aggregate all of the change activities and validate that the changes actually took place.
- **Report**—Service delivery systems should communicate change results, time to completion, and policy violations associated with the changes.

Service delivery strategies can widen service management processes within IT personnel activities to comprehensively execute management while increasing efficiency, reliability, and security through automating and directing personnel actions that support IT. Service delivery strategies also improve ongoing business operations by documenting user and applications activities throughout the enterprise IT infrastructure, resulting in a comprehensive view of data center activity. This detailed view results in more timely, efficient, and more perceptive forensics when incidents occur. This data can also be used to measure general availability and performance.

 Business unit operations each have unique procedures. These procedures and corresponding IT functions should be used to manage and direct the data center activities. Such cooperation between business and IT operations will result in focusing the efforts of IT personnel on high-priority tasks that need human insight while automating regular and low-priority activities.

Improving Profitability Through People and Technology

Organizations must focus on the people and policies that support IT. Historically, consideration of how personnel actions affect service delivery and management did not occur. Implementing procedures that are consistent, enterprise-wide, and efficient will empower the IT organization with the tools and means to guide and manage their actions with full consideration of business impact, create greater accountability, and ensure improved reliability, efficiency, and security for the IT infrastructure. Ultimately, the IT area will be able to maintain and grow profit margins for the organization while creating tangible, observable value for enterprise management as well as develop alignment between business objectives and IT service delivery.

☞ Identify significant assets, interdependencies, and vulnerabilities of critical information networks, then develop and implement realistic programs to remedy the vulnerabilities while continuously updating the assessment and remediation effort.

Incorporating IT Management and Security into the Enterprise Mission, Goals, and Processes

To successfully prepare a defense for critical enterprise IT systems and computer networks, perform a thorough assessment of the potential critical infrastructure system assets, interdependencies, and vulnerabilities. Document all such assets. Continue to assess vulnerabilities and threats that may disrupt the critical infrastructure.

Many, if not most, IT systems are highly vulnerable to intrusions, especially those assisted by, or performed by, insiders. Unauthorized intrusions occur frequently despite the widespread use of firewalls and password systems.

☞ Activities that are key to identifying vulnerabilities on the enterprise network include:

- Identify and determine the criticality of information and IT assets based on business mission criteria
- Analyze shared interdependencies within business units and throughout the enterprise
- Assess network vulnerabilities based on identification of critical assets and shared business interdependencies
- Evaluate the success of mitigation efforts by using experts outside of the IT area to ensure independence of findings
- Use leading information security practices and standards (such as Information Technology Infrastructure Library—ITIL, Control Objectives for Information and related Technology—COBIT, and International Organization for Standardization—ISO 17799) to assist in efforts to identify and address vulnerabilities

IT evolves very quickly. IT security programs and plans implemented a year ago will likely have little relevance to the technologies available now. As networks change, new vulnerabilities are introduced. As they explore systems, network intruders discover vulnerabilities that were not previously known. Organizations need a continuous process to review the new vulnerabilities, protections, standards, and recommended practices as they become available.

🔴 Special attention must be given to the possibility of single points of failure that result from a technology change, such as a firewall, critical network router, or one server hosting a mission-critical application.

Using a Shared Service Implementation Program to Protect Information and IT Assets

Effective management of information and IT is necessary for the business success of the organization. The criticality of IT is created by the:

- Increasing dependence of business operations on information and the systems that deliver the information
- Increasing number of IT and human vulnerabilities and threats
- Scale and cost of the current and future business investments in information and information systems
- Potential for technologies to dramatically change organizations and business practices, create new opportunities, and reduce costs

For many, if not most, organizations, information and supporting technology represent the most valuable business assets. Business management has high expectations for IT delivery functions in today's extremely competitive and rapidly changing business environment.

Business management has high expectations for IT delivery. Management expects:

- High quality, functionality and ease of use for IT
- Decreased delivery time for supporting IT functions
- Continuously improving IT service levels
- Lower IT costs

Most organizations understand technology can yield business operations benefits. However, many do not realize the risks involved. Successful organizations must understand and manage the risks associated with supporting existing technology and implementing new technologies. IT-related risks must be well managed to successfully secure business assets and meet regulatory and contractual requirements. Managing IT risks is a key part of enterprise governance.

IT governance should be seen as a framework built of the relationships and processes that direct and control the organization to meet goals. IT governance will add value and promote the attainment of goals by balancing risks with IT process implementation. IT governance will help ensure efficient and effective measurable improvements that are communicated to organization processes. Effective IT governance will link IT processes, security, resources, and information to organization-wide strategies and objectives.




Integrating leading accepted practices for planning, organizing, acquiring, implementing, delivering, supporting, and monitoring IT performance into the IT governance framework will ensure IT supports business objectives. As a result, the organization will maximize benefits of the information being processed and gain a competitive advantage.

Organizations must comply with quality, fiduciary, privacy, and security requirements for all their business assets, including information. To be successful and profitable, businesses must optimize all resources, including information, applications, technology, facilities, and people.

Balancing IT Security Activities with Business Assets and Operations


Organizations must always keep in mind that the primary goal of technology is to support the business. A critical goal of IT security is to protect business assets. To effectively do so, business needs must be balanced with IT security. Care must be taken to ensure IT security does not have a negative impact on business.

For example, implementing systems security patch management procedures is critical for ensuring networks are kept secure. However, the manner in which such patch management procedures are implemented must be handled in such a way that the business is not negatively impacted, or at least, minimally impacted. Historically, poorly implemented patch management procedures did not consider business impact and as a result, patch volumes and frequency, resource availability, and operational impact often negatively affected the business operations. Growing technology vulnerabilities mean IT operational teams must patch a growing number of systems and applications more frequently, in less time, and with the same resources, if not fewer.

 Patches and hotfixes can have unexpected impacts, results, and effects, such as application failures, server crashes, and network outages.

To ensure effective patch management that protects business information assets while supporting business operations, IT operational teams need to implement procedures working with business in the following manner:

- Agree on a patching policy and timeline. Don't be vague in the timeline issue. The business units can interpret "in a timely manner" very differently than it is interpreted by the IT area.
- Implement an automated technology for patch management. There are many automated options: desktop-management suites, update-aware OSs, and specialized patch-management solutions, to name a few.
- Document what is on the network. You must know what is there to patch it. Organizations that use an asset-identification process and a strong policy for quarantining or removing unknown assets are more likely to keep the business assets safe.
- Prioritize deployment of patches. It is unrealistic to believe that everything can be patched immediately with zero downtime. Classify critical assets and prioritize the order for implementing patches to help ensure deployment occurs with as little downtime as possible, and most certainly so it avoids enterprise-wide operations failure during critical business times. It is critical to test patches before deployment to the production network.
- Increase asset security by using tiered defenses. Much has been written about using a "defense in depth" strategy, but few organizations truly have multiple tiers of defense. Such layers of security will help to protect business assets in the interim until patches can be applied. Remember, a single technology cannot render a network bulletproof against security threats.
- Have a well-documented and tested backup plan. If you have a critical exposure or crippling security incident, make sure you have plans that will address a partial, or whole, network outage. Determine who should be authorized to disable critical portions of the network. Know if and how systems and network segments can be effectively quarantined within an acceptable timeframe.

 Examples of IT security requirements that must be implemented in such a way that business operations are not impacted negatively include, but are not limited to:

Security patch management

Malicious code scanning systems

Firewalls

Software, systems, and applications upgrades

Authentication systems

VPNs

Encryption


To balance IT security with business processes to effectively secure assets, organizations must perform a risk assessment. A risk assessment will allow the organization to apply security controls based on risk and not interfere with business processes. At a high level, the steps for performing a risk assessment include:

- Determining asset values and determining the consequences of losing those assets. Determine the value of the asset not only to your organization but also to potential intruders or adversaries.
- Identifying and characterizing the threats to specific assets. Address threats to the asset in as much detail as possible based upon the business and customer needs.
- Identifying weaknesses in the asset that may be exploited. Vulnerability assessments can help identify weaknesses in assets that may be exploited. Altering the nature of the asset itself can then potentially reduce risk levels. Keep in mind, though, that cost is a significant factor in such decisions, and design changes could be expensive and impact other business units or operations.
- Identifying countermeasures, costs, and tradeoffs. There will often be multiple countermeasures and controls of varying costs and effectiveness available to protect assets. There will be a point beyond which adding controls will raise costs without significantly increasing asset protection.
- Determining the results of the risk assessment. Consider asset values, threat analysis, vulnerability assessment results, likelihood, and countermeasures to then make decisions for controls to implement based upon these business considerations.

Securing the Complete Enterprise

It is critical for the entire enterprise to be considered when securing information and systems assets. Beyond IT security, the physical protection of information, assets, and personnel is fundamental to any security system. IT security safeguards are closely related to physical security by the ways in which they are used to protect certain facilities against intelligence collection or observation. Personnel security procedures are often implemented through technical means to monitor and control physical access to facilities and material.


Organizations should apply physical, technical, and procedural security consistent with the same basic risk management principles previously described. Security standards should provide uniform degrees of protection for information assets throughout the enterprise. Decisions to adopt special protection safeguards should be based upon risk management analysis of the value of the asset, the threats and vulnerabilities, and the costs of protection.

 The relationship between IT and business unit operations should be a problem-solving partnership that maximizes reciprocity.

Organizations must ensure no critical systems or assets are left unprotected. This task can be accomplished through comprehensive and consistent security management coverage across all enterprise platforms. Consistent and standard security tools—such as malicious code protection software, firewalls, switches, routers, VPNs, intrusion detection and prevention systems, access controls, strong authentication systems, and so on—must also be used throughout the enterprise to successfully protect assets.

IT must ensure that all vulnerabilities identified during the risk assessment are adequately addressed in ways that continue to support and promote business operations. In most organizations, these vulnerable points will include:

- Access points to the enterprise network
- Mobile and wireless computing
- E-commerce applications
- Internet connectivity
- Change management
- Physical security
- Personnel errors resulting from lack of training and awareness
- Business partner practices

 Organizations must address multiple security challenges throughout the enterprise. To be most effective, create asset risk posture reports regularly using a sustainable and repeatable process. To help ensure no topics are left out, base the risks being analyzed and reported upon international standards and control topics such as those found within COBIT and ISO 17799.

Up-to-date and comprehensive documentation of information assets are key to enabling meaningful asset risk posture reports. Such reports should incorporate the documentation to clearly communicate:


- Access points to the network
- Mobile and wireless computing systems
- Internet use and connections
- Vulnerability and patch management status
- Systems software versions and version control activities
- Applicable regulatory and contractual requirements for each of the systems
- Awareness and training activities
- Physical security mechanisms in place to protect information assets
- Information asset classifications and sensitivity levels


Reporting the Big Picture

Information security risk posture reports need to show the big picture end-to-end state of enterprise security. Such reports must clearly communicate to IT areas and to business unit managers where critical information assets are located, threats that exist for those assets, and the activities that are occurring to address the risks. Such reports must include details for how third-party and business partner connections and systems used to process organizational assets are secured.

Simplify Security to the Amount Necessary to Support Business

Organizations are increasingly, and sometimes entirely, dependent upon IT to support and enhance the business processes required to meet organizational goals. IT services often form the basis for the entire business model. Unfortunately, despite the importance of IT, intense competitive and economic business pressures many times result in corporate mandates to maintain, or even to decrease, current IT budgets—an occurrence that takes place often simultaneously with increased expectations for IT quality, innovation, and value. As IT grows in significance for most organizations, it is necessary for IT professionals to take a business- and service-oriented approach to operations rather than the typical technology-centric approach.

 When securing information assets, the process must be simplified and made as efficient as possible to support enterprise business operations.


 IT service management must deliver and support IT services that are implemented directly to support the organization's business requirements. It is essential that an organization's IT services support core business activities as well as facilitate change as businesses evolve and compete globally. IT must become a primary stakeholder in the business decision-making process.

To be successful, IT and business unit management must work together to implement a process by which IT always considers business operations when making decisions, and likewise, business units always consider IT issues when making business service and product decisions.

Bringing IT Value to Business Units

IT must focus on directly supporting the business objectives of the organization and emphasizing the business value IT provides to successfully establish credibility and elevate strategic impact within the enterprise. IT staff will enable new ways of doing business and will be better managed when they are involved with and are seen as an important business success contributor to the development and execution of critical business strategies. IT must demonstrate how its services make specific, tangible, and critical contributions to achieving business goals. IT groups must also show how they are achieving the levels of security, efficiency, reliability, and nimbleness that businesses need.

IT must be more proactive than what has been typical in the past. Traditionally, IT was seen as a significant, possibly strategic, investment, but not one expected to drive business value. However, the benefits were often not documented or quantified because there was no evaluation or reporting mechanism in place.

 IT can enable significant business value and efficiency in areas such as sales and customer support as well as in the traditional business operations. To do so effectively, IT areas must accept and understand a range of business terminologies, methods, techniques, and concepts that they may have historically not considered.

IT staff must consider the business operations and identify ways in which IT services can enable business to operate more efficiently and profitably. Table 2 illustrates a few examples of how such an exercise may be documented.


IT Activity	Benefit	Activity Cost
Security	Ability to protect information assets to ensure continued business processing, protect customer and mission-critical information, and comply with applicable legal and contractual requirements	Cost per security control, tool, and incident
Help desk	Ability to build Help desk staff increases into project budgets (capital expenditures) based on estimates of new user/new incident volumes, thus preventing productivity losses when users suffer system- or service-related work stoppages and Help desk is not adequately staffed to handle the request volume	Cost per incident per user
Systems administration	Ability to provide operational cost estimates to keep applications/systems up-to-date once in production	Cost per change type (major, standard, and so on)
Monitoring	Ability to demonstrate value to the bottom line provided by problem resolution effectiveness and by preventative measures	Cost per minute/hour of downtime per application

Table 2: Examples of how IT can identify ways in which their services can enable business to operate more efficiently and profitably.

Using Leading Practices to Simplify the Information and IT Security Process


In today's complex information processing environments, it is necessary to create and implement an IT security and control reference framework. To be successful, organizations must have an appreciation and understanding of the risks and threats that exist within IT as well as throughout the enterprise, to be able to effectively establish security directions and adequate controls.

Organization management must decide the amount of resources to reasonably invest for IT security and controls throughout the enterprise and balance the control and risk investments within what is a typically unpredictable IT environment. Management has an important task in determining the level of risk they are willing to accept.

 IT systems security and controls can help manage risks but they cannot completely eliminate them. Additionally, the exact levels of risk can never be determined because of the uncertainty involved with information management and processing systems.

To assist management with this difficult decision, generally accepted IT security and control standards and leading practices can be used to benchmark the organization's existing and planned IT environment. Leading practices have been developed over the years to govern IT, incorporating monitoring and reporting activities to determine the effectiveness and efficiency of the implemented controls. Such leading practices are created to support business objectives and processes.

Two of the most popular sets of worldwide control standards include ISO 17799 and COBIT. ISO 17799 is used primarily by security practitioners and contains recommendations for 10 primary areas of security concern. COBIT is used primarily by auditors, but it is also employed by managers and end users, and includes four domains containing recommended control objectives and processes for security assurance.

 The challenge organizations face when using such standards is that, with the exception of the more general Organization for Economic Cooperation and Development (OECD) principles, they are so massive and stringent that few organizations make it all the way through the requirements, let alone dedicate the time and resources necessary to become completely compliant with any one of them.

Organizations can use the most applicable standards common across the standards as a basis for information governance controls. Many overlaps are discovered upon examination of two of the most commonly used standards.

BS 7799 and ISO 17799


British Standard (BS) 7799 (see <http://www.iso.ch>) sets the requirements for an Information Security Management System and is recognized and used worldwide. The requirements “help identify, manage, and minimize the range of threats to which information is regularly subjected.” The BS 7799 Information Security Management Standard is published in two parts:

- ISO/IEC 17799 Code of practice for Information Security Management (commonly referenced as ISO 17799)
- BS 7799-2:2002 Specification for Information Security Management

This standard is process driven and technology independent. It was developed by a consortium of companies and information security practitioners throughout the world and describes best practices for information security in 10 operational areas (see Figure 2).



Figure 2: ISO 17799 control modules.

 The ISO 17799 standard gained widespread recognition following publication by the ISO in December 2000. Formal certification and accreditation were introduced around the same time.

COBIT

COBIT (see <http://www.isaca.org/cobit.htm>) serves as a framework of generally applicable information security and control practices for IT control and is recognized and used worldwide. The report can be ordered from the Information Systems Audit and Control Association (ISACA) by phone or mail.

The COBIT framework strives to help management benchmark the security and control practices of IT environments, allows users of IT services to be assured that adequate security and control exists, and allows auditors to verify their opinions on internal control and to advise on IT security and control matters. The primary motivation for ISACA to provide the framework was to enable the development of clear policy and good practices for IT control throughout the industry worldwide. It consists of four primary operational domains, each with multiple identified control processes.

The COBIT framework strives to bridge the gaps between business risks, control needs, and technical issues by providing good practices across a domain and process framework. COBIT helps to optimize information investment by supporting business processes and showing how each individual control activity satisfies the information requirements and impacts the IT resources. Management, through enterprise governance, must ensure that due diligence is exercised by all individuals throughout the organization for the use, design, development, maintenance, or operation of information systems (see Figure 3).

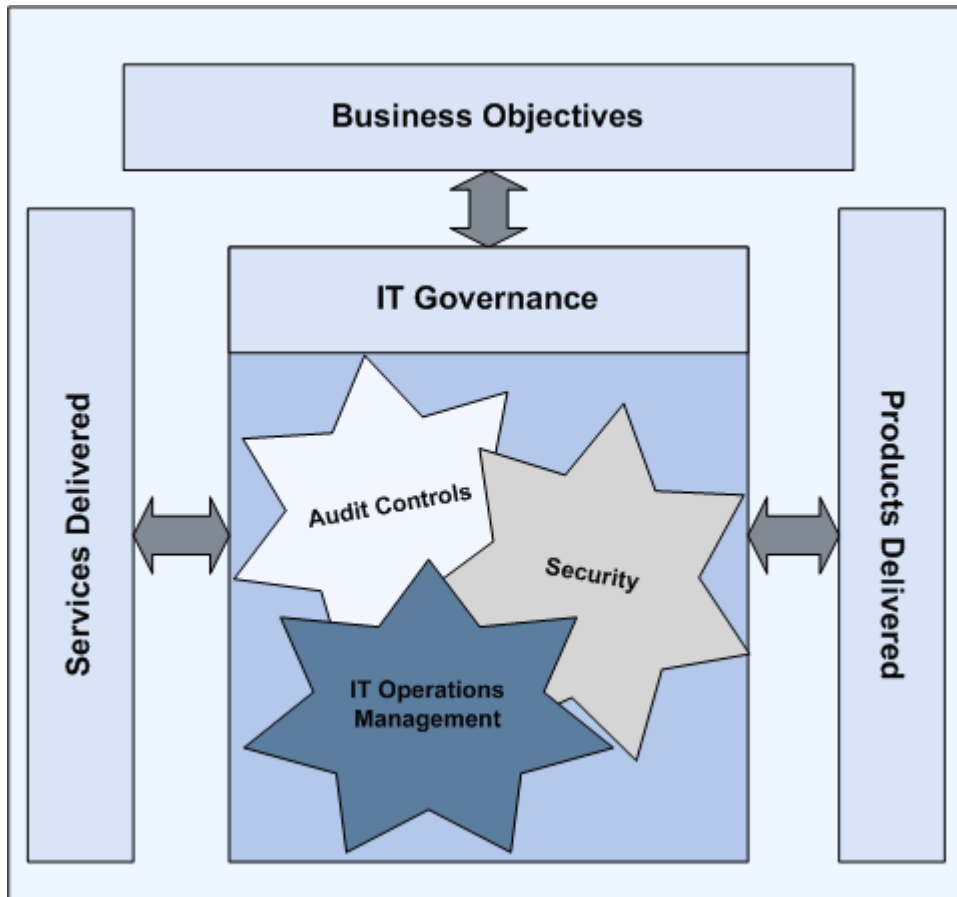



Figure 3: The COBIT framework.

 COBIT was first published in 1996 and is now in its third edition. COBIT is one of the most popular and internationally accepted sets of guidance materials for IT governance.

Quickly Comparing COBIT and ISO 17799

COBIT is an IT governance and control framework that consists of four broad domains containing 34 high-level control objectives and 318 detailed control objectives.

BS7799 (the first part of which is equivalent to ISO 17799) focuses on information security with 127 controls within 10 domain areas.

COBIT is a broader framework that applies to a wider range of information handling activities beyond security. However, it can incorporate BS7799/ISO17799 for security-related issues, whereas the other way it might be almost impossible.

Certification is another significant difference; BS7799 implementation can be certified. Currently there are no certifications available for COBIT.

Reducing and Eliminating Unnecessary Information Collected Through Network Security Monitoring

An important part of IT asset security is monitoring the IT network components for variances that indicate potential problems or incidents. Effective security monitoring will provide the ability to review and evaluate network information related to security in a timely manner to allow for an efficient and effective response to minimize potential information asset damage.

Monitoring does not consist of simply looking at audit reports and reviewing security alerts. Waiting for an alarm is reactive, and most likely damage has already occurred. Effective monitoring is more proactive and involves looking at the available forms of information generated through various network information and reports, then feeding that information into a larger repository and a decision tool that IT security personnel can utilize.



A well-designed and managed monitoring system will improve the productivity of the security manager as well as reduce the level of effort it takes to identify weaknesses before they become problems.

The challenge in most organizations is determining what to log, how much to log, and how long to keep the logs. The information gathered through monitoring should lower the risk to the business through improved response and faster reaction to an incident.



What is it worth to know more information than that which will lower risk to IT assets? Is it worth it to know there have been additional policy violations? Remember, proactive security can only be quantified in terms of potential loss through preventive and detective measures, including information gathered through monitoring tools.

To be most efficient in time, and most productive and successful in identifying security-related irregularities, organizations should

- Automatically filter, normalize, and correlate collected data from multiple sources, then accumulate the data in a central location
- Filter normal events and reduce irrelevant alerts based upon results of risk assessments
- Identify the key events that require the attention of IT operations, then document and rehearse what to do should the events happen

Results of security monitoring should be analyzed, summarized, and reported to management throughout the organization who are impacted by the associated IT assets. It is important to make security challenges and issues related to the information gathered understandable to business unit management. Clearly report information and systems assets and corresponding controls.



Security monitoring is not an endpoint but must be part of the overall strategic plan for security in business. As part of that plan, the costs and benefits of monitoring must be considered in the decision process. Effective security monitoring and reporting are important components for sustaining asset protection on an ongoing, consistent basis.

Implementing Service-Driven Security Controls


After identifying information assets, threats, and controls, use an ongoing process to automatically address as many security issues as possible through the most efficient ways available:


- Manage security by business service rather than by IT platform
- Provide end-to-end security in a way that makes sense for your end users and supports their business processes
- Make security management as efficient as possible
- Demonstrate due diligence in implementing security
- Incorporate IT security into the IT governance framework to successfully secure information assets
- Relate security issues to business processes and products
- Define the role the IT service Help desk will have with regard to security
- Make ongoing security management a sustainable consistent process
- Measure security controls' effectiveness and management awareness
- Stay aware of new security risks and related security monitoring tools and techniques

Using IT Operations Frameworks for Service-Driven Controls

Using an IT operations framework to implement service-driven security controls will not only facilitate the management and operation of the IT infrastructure but also effectively incorporate security activities into the business processes. An IT operations framework can be applied within organizations of all sizes. Internationally used IT operations frameworks have grown in popularity from when they were first introduced in the 1980s. At that time, technologies were expanding out through organizations that were formally mainframe-centric and quickly becoming decentralized and distributed throughout all business units. These business units often took it upon themselves to install and use their own file servers and mini-systems. As a result of this lack of centralized oversight and standardization of OSs and practices, turmoil, problems, and inefficiencies often occurred. The use of IT operations frameworks helped to address the many concerns.

An IT operations framework can be applied anywhere within the organization environment and then expand out into other areas. IT operations frameworks can be applied incrementally, adding more components as the organization matures in its operating capabilities.

 A key component is defining the set of roles that encompass the full range of activities involved in operating an IT infrastructure. An effective IT operations framework will group together common IT processes throughout all stages of the IT life cycle and associate them with the relevant roles, while at the same time ensuring appropriate separation of duties.


 IT security, using controls such as those recommended within COBIT and ISO 17799, can be infused within the processes to effectively manage asset security.

The steps in establishing an IT operations framework include:

- Understand the current organization's operations strengths and weaknesses
- Prioritize goals for operations improvement
- Implement one or more service improvement projects (SIPs) to upgrade the capabilities within the desired IT service functions

Considering Internationally Used IT Operations Frameworks

An IT operations framework provides a method for maintaining your IT organization, systems, and processes. It can help reduce costs, inefficiencies, and downtime. However, communication about how the framework should be used is important because those who are unfamiliar with them can perceive frameworks poorly.

 It is important for successful implementation of a framework that consensus is obtained throughout the enterprise from all areas that use the technology.

To gain consensus for implementation:

- Explain the IT operations frameworks in a common, non-technical and business-focused, language
- Explain and raise awareness of current problems
- Leverage work that has already been done

Important to success, as with any IT initiative, is obtaining buy-in and support from senior management as well as effectively communicating to middle management the primary objectives of implementing such a framework.


☞ Explain a common but detailed business process that your company executes, such as a new product release. Show how IT enables this process through technology services, such as marketing through Web presence. In addition, show how these services rely on standard operating procedures to be well documented, reliable, and current. This exercise will help communicate the continuous delivery of service from IT to the business.

To help explain the framework at a high level and obtain management understanding, it helps to present the concept in a clear, simple way that is easy for management that has little to no technology background to understand. One way to do so is by mapping business functions to IT services, security, and operations. Table 3 provides a high-level example of how to do so for an online financial application system.

Business Process	IT Services	IT Security	IT Operations
Product marketing	Web presence and CRM campaigns	Information privacy, transaction security, regulatory compliance	Content management and reporting
Application release	Application development	Risk assessment and access controls	Project management, release management, change management, configuration management
Customer support	Call center	Customer identity authentication and privacy controls	Incident management, problem management, systems management

Table 3: Online financial application system from business to IT operations.


The goal of creating and communicating such a table is to demonstrate that IT services rely upon common operational tasks. It will also help business managers to realize that most of the IT tasks will be the same even for different business processes. For example, a different business process may use a different server in a different data center and perform a different function, but it will be changed by using controlled consistent procedures, logging the new configuration, updating systems monitors, and informing the Help desk.

 Organizations must change their perception of IT. In the past, business units typically just considered whether IT could get something done for their business operations in the shortest amount of time. Business management must start considering what IT activities will need to occur to accomplish business operations.

Working with a framework will be more of a coordination of current work than a redesign of all work. Most organizations will be able to fit existing projects into an operations framework, then leverage mutual experience and effort to realize these goals faster.

Using ITIL

The United Kingdom government's Central Computer and Telecommunications Agency (CCTA) originally created ITIL in 1989 to advise government agencies about how to make best use of technology. ITIL was created as a series of books describing how to effectively and consistently deliver IT services by following best practices. The core of the approach was to apply established principles of management science to mass usage IT.

 ITIL is now the most widely accepted approach to IT service management in the world. ITIL's current library provides a comprehensive and consistent set of best practices for IT service management to help ensure quality and achieve business effectiveness and efficiency when using IT.

ITIL contains a comprehensive, non-proprietary, publicly available reference model for IT management processes, job descriptions, and control mechanisms. ITIL was compiled by using the combined experience of commercial and governmental practitioners worldwide. ITIL is now the standard used for managing IT by some of the world's leading businesses, such as Microsoft, Procter & Gamble, and ABN AMRO in addition to many government agencies. The repeatable documented processes improve IT service delivery and management.

Organizations have indicated the following benefits of using ITIL:

- IT services better meet business requirements because IT activities are directed to supporting the organization in achieving strategic objectives
- IT service delivery efficiency and quality is improved
- IT service delivery and support priorities are clearly documented and understood
- Relationships between business units, customers, IT, and vendors are improved
- Communication between the IT and business areas are improved through improved service level management
- Areas with process weaknesses are more quickly identified through monitoring service delivery

ITIL is organized into a series of sets, each of which is divided into two main areas:

- Service Support is the practice of those disciplines that enable IT services to be provided effectively.
- Service Delivery is managing the IT services themselves to ensure that they are actually provided as agreed between the service provider (IT) and the customer (business units).

The ITIL Service Support Process Model is composed of six disciplines:

- Incident Management—To restore normal service operation as quickly as possible with minimum disruption to the business and ensure that the best levels of availability and service are maintained.
- Problem Management—To minimize the negative business impact of incidents and problems caused by errors in the infrastructure and to proactively try to prevent the incidents, problems, and errors.
- Change Management—To ensure that standardized methods and procedures are used for efficient and prompt handling of all changes, minimizing the impact of any related incidents upon service and business activity.
- Release Management—To relate change holistically to an IT service and ensure that all aspects of a release, both technical and non-technical, are considered together.
- Configuration Management—To provide a logical model of the IT infrastructure by identifying, controlling, maintaining, and verifying the versions of all configuration items being used.
- Service/Help Desk—To provide a single point of contact for end users who need help by focusing on incident control and communication.

The ITIL Service Delivery Process Model is composed of five disciplines:

- Service Level Management—To maintain and improve business-aligned IT service quality through a constant cycle of agreeing, monitoring, reporting, and reviewing IT service achievements in addition to performing actions to eliminate unacceptable levels of service.
- Availability Management—To optimize the capability of IT infrastructure and supporting organization to deliver a cost-effective and sustained level of availability that enables the business to fulfill objectives.
- Capacity Management—To understand future business requirements (the required service delivery), the organization's operation (the current service delivery), and the IT infrastructure (the means of service delivery), and ensure that all current and future capacity and performance aspects of the business requirements are provided cost effectively.
- IT Financial Management—To provide cost-effective stewardship of IT assets and financial resources used in providing IT services.
- IT Service Continuity Management—To support the overall business continuity management process by ensuring that the required IT technical and services facilities can be recovered within required and agreed-upon business time scales.

Figure 4 shows an overview of the ITIL corporate IT organization books.

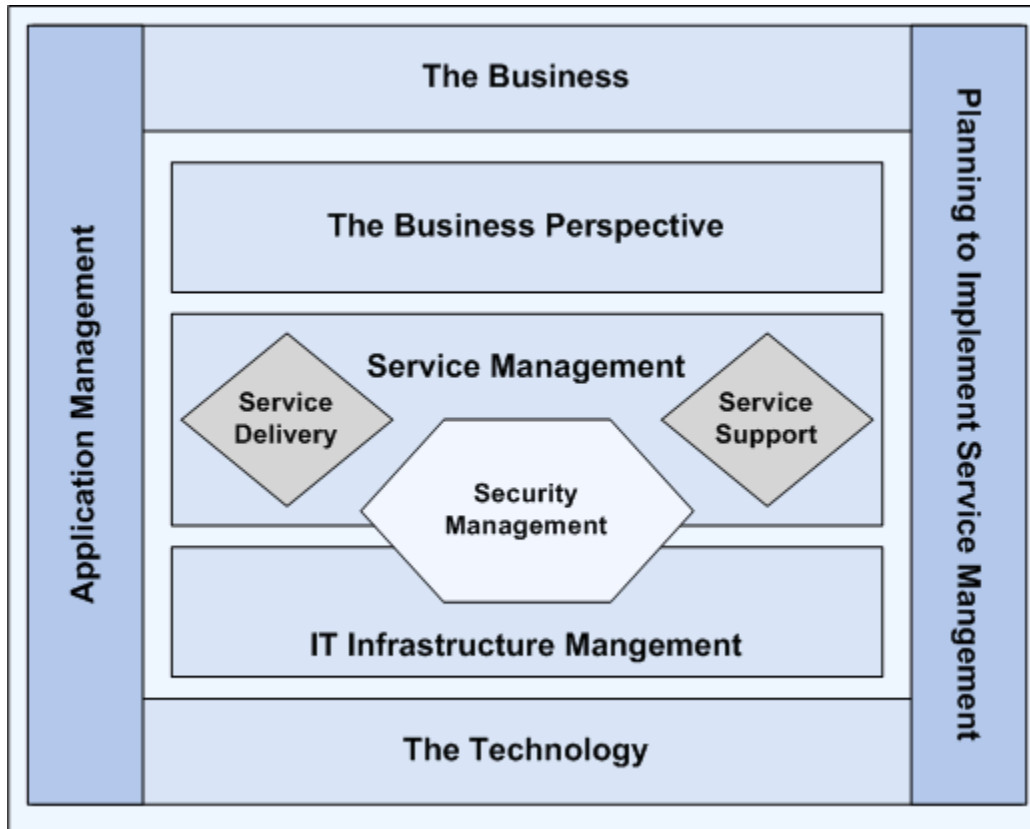


Figure 4: ITIL corporate IT organization books.

For more information about ITIL, see <http://www.itil.co.uk/>.

Using the Microsoft Operations Framework

The Microsoft Operations Framework (MOF) was first introduced in 2000. MOF combines the ITIL standards with specific guidelines for using Microsoft products and technologies in addition to extending the ITIL code of practice to support distributed environments and industry trends such as application hosting and Web-based transactional systems.

The foundation elements of MOF include:

- The Team Model
- The Process Model
- The Risk Management Discipline

These elements provide guidance for managing the people, processes, and risks involved in IT services, focusing on enabling technologies and promoting best practices to achieve high system availability, reliability, supportability, and manageability; all directly applicable to Microsoft platforms. However, they also provide guidance on interoperability with other technology platforms.

The MOF Process Model follows four principles:

- Structured architecture that must provide an order for all operational activities addressed during mission-critical computing. This architecture must provide for process integration, life cycle management, mapping of roles and responsibilities, and overall management oversight and control. It also must provide the foundation for process automation and technology-specific operations.
- Rapid life cycle, with iterative improvement that supports the ability to incorporate change quickly as well as to continuously assess and iteratively improve the overall operations environment. The MOF Process Model categorizes key operational activities, with the activities occurring in parallel, 24 hours a day, seven days a week.
- Review-driven management that includes high-level operations management reviews at key points within the life cycle. The reviews will then be used to evaluate performance for release-based activities as well as steady state, or daily, operational activities.
- Embedded risk management addressing risks within the context of each process and role.

Comparing MOF to ITIL

MOF aligns and builds on the IT service management practices that have been documented within ITIL. Microsoft has been involved with the ITIL community since 1999, both using the ITIL content and contributing to new and updated documentation, including co-authoring several books. Microsoft states one goal of MOF is “to extend and enhance the practices and guidance offered through ITIL in order to provide more detailed prescriptive guidance in specific areas of IT management.”

MOF is similar to ITIL in several ways:

- MOF and ITIL address the full IT life cycle.
- MOF and ITIL are both based on best practices for IT management and incorporate expertise of international practitioners.
- MOF and ITIL disciplines are applicable across the business community, from small businesses to enormous enterprises.
- MOF and ITIL include more than just a documentation set. A variety of resources have been developed to support MOF and ITIL principles and guidance, including self-assessments, IT management tools that incorporate MOF and ITIL terminology and features, training programs, and consulting service offered by numerous third-party vendors and consultants.



MOF expands upon ITIL by adding team and process models and risk management and service delivery functions. ITIL has been used for a much longer time and by more organizations, and has been continuously refined and improved.

Building an Asset Security Roadmap

Information security standards—such as ISO 17799, control objectives—such as COBIT, and IT operations frameworks—such as ITIL, can be combined to successfully incorporate IT asset protection into organization-wide asset protection. Incorporating such best security and control practices into the management framework will put security in context with the rest of the business processes and will in effect create an asset security roadmap.

By incorporating these ISO 17799 and COBIT best practice standards and controls into an IT governance framework such as ITIL, organizations will:


- Improve the ability to audit IT
- Improve business operations and customer care systems and processes
- Make multi-vendor operations feasible and as seamless as possible
- Improve information and IT asset security
- Smooth legacy systems integration
- Make management of distributed computing practical and cost-effective
- Enhance management tool requirements, selection, and implementation
- Improve service level agreements
- Improve organizational effectiveness
- Enable evaluation and improvement of operational practices
- More effectively identify and implement management tools
- Clearly define IT and business roles and responsibilities

Putting It All Together

To begin putting all of this information into practice, start by looking at more detail within each of the ITIL disciplines. As you look within the disciplines, map each of the applicable COBIT controls and ISO17799 security standards.

Configuration Management

- Details the provision and management of the organization's IT services
- Details the maintenance, movement, and problems experienced with the configuration items
- Details the items upon which the organization's IT services are dependent, including hardware, software, documentation, and personnel
- Specifies and identifies all IT components
- Specifies who is authorized to manage, control, and change each configuration item
- Records the status of all configuration items and how they are maintained
- Reviews and audits information within the configuration management database to verify accuracy

 All configuration items within an organization's IT services must be defined to identify the items that are used for each IT service. Without such definition, critical configuration items could be compromised, misplaced, lost, stolen, moved, or otherwise inappropriately used, resulting in a negative effect on the availability of the services dependant upon them as well as enabling the use of unauthorized items in the provision of IT services.

Relates to ISO 17799 standards:

- 4.2 Security of Third Party Access
- 8.7 Exchanges of Information and Software
- 10.4 Security of System Files

Relates to COBIT Delivery and Support controls:

- 9.1 Configuration Recording
- 9.2 Configuration Baseline
- 9.3 Status Accounting
- 9.4 Configuration Control
- 9.7 Configuration Management Procedures

Incident and Problem Management

- Resolves and prevents incidents that affect normal IT services activities
- Ensures IT services faults are corrected and helps prevent fault recurrence
- Applies preventative maintenance to help reduce the likelihood of faults from occurring

Effective incident and problem management will ensure IT services availability is maximized and will help to protect the integrity and confidentiality of information by identifying and addressing the causes of problems.

Relates to ISO 17799 standards:

- 8.1.3 Incident Management Procedures
- 4.2.2 Security Requirements in Third-Party Contracts
- 8.4.3 Fault Logging


Relates to COBIT controls:

- 5.11 Incident Handling
- 10.1 Problem Management System
- 10.2 Problem Escalation
- 10.3 Problem Tracking and Audit Trail
- 10.4 Emergency and Temporary Access Authorizations
- 10.5 Emergency Processing Priorities

Change Management

- Ensures that all changes to IT services configuration databases and fields occur following established plans and with authorization
- Ensures there is a business reason for each configuration change
- Identifies the specific configuration items and IT services affected by each change
- Ensures documentation for planning and testing the change
- Ensures that a back out plan exists in case the change results are unexpected

IT security must be embedded into the change management process to ensure that all changes are assessed for risks prior to the change. This requirement includes assessing the potential business impacts in the event that the change produces undesirable results.

 If change management procedures are not effective, unauthorized changes to IT services could occur, which could have major impacts on the business, including financial loss, customer loss, market loss, litigation, and in the worst case scenario, even collapse of the business that the IT services are there to support.

Relates to ISO 17799 standards:

- 8.1.2 Operational Change Control
- 10.5.1 Change Control Procedures
- 10.5.2 Technical Review of Operating System Changes


Relates to COBIT controls:

- 5.7 Testing of Changes
- 6.1 Change Request Initiation and Control
- 6.2 Impact Assessment
- 6.3 Control of Changes
- 6.4 Emergency Changes
- 6.5 Documentation and Procedures

Service/Help Desk

- Provides a first contact for business users in their use of IT services when something does not work as expected
- Provides a single point of contact for end users who need help, creating efficiencies for operations that will help prevent asset and resource losses
- Provides a central location to receive all calls and emails about IT incidents, record all incidents, prioritize incidents, classify and escalate incidents, determine ways to continue working during an incident, update end users about incident progress, handle communications for IT processes, and provide update reports to management, process managers, and business units about service desk performance

There are two basic types of service and Help desks. One type provides a simple call logging function and escalates calls to more experienced and trained staff. The other type provides a high degree of business and technical knowledge with the ability to resolve many, or even most, incidents at the time when business user reports them. Businesses need to choose which type to use based upon what their business requires.

 Because the service or Help desk is typically the first contact business personnel have when reporting an IT incident or problem, service or Help desk staff must possess skills and experience to help prevent recurrence of incidents and initiate measures that will limit the impact of any breaches or incidents within IT security.

Relates to ISO 17799 standards:


- 6.3.2 Reporting Security Weaknesses
- 6.3.3 Reporting Software Malfunctions

Relates to COBIT controls:


- 8.1 Help Desk
- 8.2 Registration of Customer Queries
- 8.3 Customer Query Escalation

Release Management

- Details the management of all software configuration items within the organization
- Establishes responsibility for the managing software development, installing and supporting the organization's software products
- Ensures that software is regarded as a tangible asset and is effectively controlled
- Controls versions of the same software within the organization
- Ensures that there are no unlicensed or illegal copies of externally provided software used within the organization
- Creates a Definitive Software Library (DSL) in which the master copies of all software is stored and from where software control and release is managed as part of an effective software control and distribution practice

 The DSL should consist of both a physical store and a logical store. Store the master copies of all software media (typically obtained from external sources) into the physical store. Use the logical store to index all software and releases and versions, document where the physical media can be located, store software developed internally, and other details.

Software control and procedures should include the management of the software configuration items and document how to distribute and implement them into the production environment. Include with the documentation a definition of the organization's release procedures, the definition of how to implement version control, and detailed procedures for how software must be built, released, and audited.

 The three key areas of IT security (availability, confidentiality, and integrity) can be put at risk as a result of inadequate software control and distribution. Poorly managed, unauthorized, and insufficiently tested software changes can lead to significant problems in the production environment, such as unavailable IT services, fraud, viruses, compromised data integrity, and malicious damage to data files—just to name a few.

Create procedures to fully review software control and distribution procedures with a security assessment to ensure that appropriate counter measures are in place to reduce the potential for threats.

Relates to ISO 17799 standards:

10.4.1 Control of Operational Software

8.3.1 Controls Against Malicious Software

Relates to COBIT controls:

6.7 Software Release Policy


6.8 Distribution of Software

Service Level Management

- Ensures that agreed upon IT services are delivered when and where they are supposed to be delivered, providing the primary management of IT services
- Provides the agreed upon IT services in a secure, efficient, and cost-effective manner
- Reviews existing IT services
- Negotiates with the business unit and partner customers
- Reviews the foundation contacts of 3third-party service providers
- Produces and monitoring service level agreements
- Implements service improvement policy and processes, including establishing priorities, and planning for service growth
- Involves the accounting process to cost services and recovering these costs where possible

A service level agreement is a critical part of service level management, from the perspective of both the supplier and the recipient. A service level agreement must clearly document and define the parameters of the relationship itself. These agreements should also include provisions for mediation.

IT security is an integral part of IT service delivery. The Service Level Management process is ultimately responsible for ensuring that IT services are provided in a secure manner as well as ensuring the availability of IT services is maximized within cost and efficiency constraints.

 Don't forget about contingency planning, which is an important part of service delivery that ensures services can be recovered and maintained when an incident occurs.

Relates to ISO 17799 standards:

- 4.2 Security of Third-Party Access
- 4.3 Outsourcing
- 6.1 Security in Job Definition and Resourcing
- 10.5 Security in Development and Support Processes

Relates to COBIT controls:

- 1.2 Formulation of Alternative Courses of Action
- 1.5 Technological Feasibility Study
- 2.3 Design Approval
- 2.8 Definition of Interfaces
- 4.1 Operational Requirements and Service Levels

Capacity Management

- Ensures that the IT infrastructure is provided at the right time in the right volume at the right price
- Ensures that IT is used in the most efficient manner
- Uses input from all business units to identify IT services that are (or will be) required, the IT infrastructure required to support these services, the level of contingency necessary, and what the cost of the resulting infrastructure will be
- Uses multiple capacity management processes, including performance monitoring, workload monitoring, application sizing, resource forecasting, demand forecasting, and modeling

Capacity management processes enable the creation of the capacity plan, forecasts, tuning data, and service level management guidelines. Perform a capacity planning function risk assessment to help ensure that the process is carried out effectively and that the findings are acted upon.

Relates to ISO 17799 standard:

- 8.2.1 Capacity Planning

Relates to COBIT control:

- 3.7 Capacity Management of Resources

Continuity Management, Disaster Recovery, and Business Continuity

- Puts plans in place and manages them to ensure that IT services can recover and continue if an incident occurs
- Implements not only reactive measures but also proactive measures to reduce the risk of a disaster or incident
- Recovers the IT infrastructure used to deliver IT services
- Ensures that the full mission-critical end-to-end business process can continue if an incident occurs

-
- Prioritizes the businesses and operations to be recovered by conducting a Business Impact Analysis (BIA)
 - Performs a risk assessment (sometimes referenced as a risk analysis) for each IT service to identify the assets, threats, vulnerabilities, and countermeasures for each service
 - Evaluates the options for recovery
 - Produces and maintains the contingency plan
 - Tests, reviews, and revises the plan on a regular basis

Continuity management is so important that your organization should not do business with IT service providers if they do not have a contingency planning practice implemented. Keep in mind that many organizations that have been involved in a disaster in which their contingency plan failed went out of business within 18 months following the disaster according to the United Kingdom Office of Government Commerce. This statistic is supported by a Gartner Group study that found “two out of every five enterprises that experience a disaster go out of business within five years” (Gartner, *Disaster Recovery Plans and Systems are Essential*, Robert Witty, Donna Scott, September 2001).

All components of continuity management (including contingency planning, business continuity, and disaster recovery) are integral parts of IT security and risk analysis. Inadequate contingency planning is a risk to the business, but is often overlooked until after a security or other breach results in the loss of supporting IT systems.

Relates to ISO 17799 standards:

- 7.1 Secure Areas
- 7.2 Equipment Security
- 8.4.1 Information Back Up
- 11.1 Aspects of Business Continuity Management
- 12.1 Compliance with Legal Requirements

Relates to COBIT controls:

- 4.3 IT Continuity Plan Contents
- 4.6 Testing the IT Continuity Plan
- 4.9 User Department Alternative Processing Back-up Procedures
- 4.12 Off-site Back-up Storage
- 11.23 Back-up and Restoration
- 11.24 Back-up Jobs
- 11.25 Back-up Storage

Availability Management

- Identifies levels of IT service availability for use in service level reviews with business unit and business partner customers
- Ensures that all areas of each IT service is measurable and defined within the service level agreement
- Measures IT service availability in the following areas that are included in the service level agreement:
 - Agreement statistics identifying activities included within the service
 - Availability of agreed upon service times, response times, and so on
 - Help desk calls, including the number of incidents raised, response times, resolution times
 - Contingency details, location of documentation, contingency sites, third-party involvement, and so on
 - Capacity measurements, including such information as performance timings for online transactions, report production, numbers of users, and so on
 - Costing details, including charges for the IT service and any penalties when service levels are not met

IT service availability is typically calculated based on a model involving the Availability Ratio and a technique such as Fault Tree Analysis. Such calculations include the following elements:

- **Serviceability**—The expected availability of a component for a service provided by a third party
- **Reliability**—The time for which a component is expected to perform without failures under specific conditions
- **Recoverability**—The time it should take to restore a component back to its operational state after a failure
- **Maintainability**—How easily a component can be maintained, including both remedial and preventative
- **Resilience**—The ability for the IT service to withstand failure
- **Security**—The ability of the IT service components to withstand security breaches

The primary focus of ensuring IT infrastructure continues to be availability for the provision of IT services. IT security is also a critical component of availability management. Perform a risk analysis to identify any resilience measures to implement for IT services, identify the reliability of service elements, identify how many problems have been caused as a result of system failure, and to be able to recommend controls, such as development standards, testing, physical security, personnel skills, and so on, to improve availability of the IT infrastructure.

Relates to ISO 17799 standards:


- 6.3 Responding to Security Incidents and Malfunctions
- 8.1 Operational Procedures and Responsibilities
- 8.5.1 Network Controls
- 11.1.2 Business Continuity and Impact Analysis

Relates to COBIT controls:

- 4.2 IT Continuity Plan Strategy and Philosophy
- 4.4 Minimizing IT Continuity Requirements
- 4.10 Critical IT Resources
- 10.1 Problem Management System
- 10.2 Problem Escalation
- 12.6 Uninterruptible Power Supply

IT Financial Management

- Ensures that the IT infrastructure is obtained at the most effective (not necessarily cheapest) price and calculates the cost of providing IT services using structured processes that allow the organization to understand the costs of the IT services and then be able to most accurately recover the costs from the business unit or business partner service customer
- Divides costs into costing units to most successfully identify costing trends and where inefficiencies exist; costing units should include equipment, software, personnel (staff, overtime, benefits, and so on), accommodation, and transfer costs of third-party service providers

 Divide IT costs into direct and indirect costs, and indicate whether each is capital or ongoing.

Effective IT financial management enables the organization to identify the amount being spent on security countermeasures provided within IT services. Effectively managing IT security costs will ultimately reflect upon the cost of providing the IT services, and potentially what is charged in the recovery of those costs. Use a Business Impact Assessment and/or risk assessment to balance the amount being spent on IT security with the risks and the potential losses that the service could incur as identified.

Relates to ISO 17799 standards:

9.4.6 Segregation in Networks

2.3 Risk Management

Relates to COBIT controls:

6.2 Costing Procedures

6.3 User Billing and Charge back Procedures

Summary

When incorporating security and controls into an IT governance framework, consider the following:

- What is your organization required to do?
- What is your organization afraid not to do? Based upon risk assessment results, recent incidents, both internal and at other organizations, and so on.
- Do the roles and responsibilities clearly document security responsibilities?
- How can the organization accomplish the security objectives in harmony with business objectives?
- What metrics and audit activities does the organization need to implement?
- How can the organization effectively achieve IT security objectives?
- What adjustments does the organization need to make?
- What is the current state of the security posture and which framework requirements must be implemented in the near-term?

Utilizing an IT governance framework to incorporate information security activities into the business processes and environment will demonstrate the value of information security to the business leaders throughout the enterprise. To facilitate your asset protection planning and work, use Appendix A to map the components of ITIL with the corresponding controls found in COBIT and ISO 17799.

Appendix A

Use the following table as an information and IT asset protection roadmap based upon an internationally accepted IT management framework and security control. For more information and to obtain the full details for each of the controls listed, see <http://www.itil.co.uk/>, <http://www.iso.ch>, and <http://www.isaca.org/cobit.htm>.

ITIL Discipline	ISO 17799 Controls	COBIT Controls
Configuration Management	<p>4.2.2 Security Requirements in Third-Party Contracts. Control access to the organization's information processing facilities by third parties. Include control requirements within third-party contracts.</p> <p>8.7.1 Information and Software Exchange Agreements. Control exchanges of data and software between organizations to prevent loss, modification, or misuse of data.</p> <p>10.4 Security of System Files. Give the user function or development group that owns the application the responsibility for controlling access to application system files.</p> <p>12.2 Reviews of Security Policy and Technical Compliance. Regularly review the security of information systems against the applicable security policies and the technical platforms; audit information systems for compliance with security implementation standards.</p>	<p>9.1 Configuration Recording. Ensure that only authorized and identifiable configuration items are recorded in inventory upon acquisition.</p> <p>9.2 Configuration Baseline. Document a baseline of configuration items as a checkpoint to return to after changes.</p> <p>9.3 Status Accounting. Ensure that the configuration records reflect the actual status of all configuration items including the history of changes.</p> <p>9.4 Configuration Control. Ensure that the existence and consistency of recording IT configuration is periodically checked.</p> <p>9.7 Configuration Management Procedures. Ensure that critical components of the organization's IT resources have been appropriately identified and are maintained.</p>
Incident Management	<p>8.1.3 Incident management procedures. Ensure a quick, effective and orderly response to security incidents.</p> <p>Security requirements in third-party contracts. Base third-party access on a formal contract referencing all the security requirements to ensure compliance with the organization's security requirements.</p> <p>6.3 Responding to Security Incidents and Malfunctions. Minimize the damage from security incidents and malfunctions, monitor and learn from such incidents.</p>	<p>5.11 Incident Handling. Address security incidents by providing an area with sufficient expertise and rapid and secure communication facilities.</p> <p>10.4 Emergency and Temporary Access Authorizations. Document emergency and temporary access authorizations using standard forms and maintain on file; ensure that these authorizations are approved by appropriate managers, securely communicated to the security function, and automatically terminated after a predetermined period.</p> <p>10.5 Emergency Processing Priorities. Establish, document, and approve emergency processing priorities by appropriate program and IT management.</p>

ITIL Discipline	ISO 17799 Controls	COBIT Controls
Problem Management	<p>8.4.3 Fault logging. Faults should be reported and logged and corrective action should be taken. Establish clear rules for handling reported faults.</p>	<p>10.1 Problem Management System. Ensure that all operational events that are not part of the standard operation (incidents, problems, and errors) are recorded, analyzed, and resolved in a timely manner.</p> <p>10.2 Problem Escalation. Ensure that identified problems are resolved in the most efficient way on a timely basis.</p> <p>10.3 Problem Tracking and Audit Trail. Provide for adequate audit trail facilities that allow tracing from incident to underlying cause and back.</p>
Change Management	<p>8.1.2 Operational Change Control. Changes to information processing facilities and systems should be controlled.</p> <p>10.5.1 Change Control Procedures. There should be strict control over the implementation of changes to minimize the corruption of information systems.</p> <p>10.5.2 Technical Review of Operating System Changes. Periodically review and test application systems when OS changes occur to ensure that there is no adverse impact on operation or security.</p>	<p>3.6 System Software Change Controls. Ensure that system software changes are following the organization's change management procedures.</p> <p>5.7 Testing of Changes. Ensure that an independent test group tests changes in accordance with the impact and resource assessment in a separate test environment before use in the regular operational environment.</p> <p>6.1 Change Request Initiation and Control. Ensure that all requests for changes, system maintenance, and supplier maintenance are standardized and subject to formal change management procedures.</p> <p>6.2 Impact Assessment. Ensure that all requests for change are assessed in a structured way for all possible impacts on the system and its functionality</p> <p>6.3 Control of Changes. Ensure that change management and software control and distribution are properly integrated with a comprehensive configuration management system.</p> <p>6.4 Emergency Changes. Establish parameters defining emergency changes and procedures to control these changes when they circumvent the normal process of technical, operational, and management assessment prior to implementation.</p> <p>6.5 Documentation and Procedures. Ensure that whenever system changes are implemented, the associated documentation and procedures are updated accordingly.</p>

ITIL Discipline	ISO 17799 Controls	COBIT Controls
Service/Help Desk	<p>6.3.2 Reporting security weaknesses. Require information services users to note and report any observed or suspected security weaknesses in, or threats to, systems or services.</p> <p>6.3.3 Reporting software malfunctions. Procedures should be established for reporting software malfunctions.</p> <p>4.1.5 Specialist information security advice. Provide an experienced in-house information security advisor to answer specific security questions.</p>	<p>8.1 Help Desk. Establish user support within a Help desk function.</p> <p>8.2 Registration of Customer Queries. Ensure that the Help desk adequately registers all customer queries.</p> <p>8.3 Customer Query Escalation. Ensure that customer queries that cannot immediately be resolved are appropriately escalated within the IT function.</p>
Release Management	<p>10.4.1 Control of operational software. Provide controls for the implementation of software on operational systems.</p> <p>8.3.1 Controls against malicious software. Implement detection and prevention controls to protect against malicious software and appropriate user awareness.</p>	<p>6.7 Software Release Policy. Ensure that the release of software is governed by formal procedures ensuring sign off, packaging, regression testing, handover, and so on.</p> <p>6.8 Distribution of Software. Establish specific internal control measures to ensure distribution of the correct software element to the right place, with integrity, and in a timely manner with adequate audit trails.</p>
Service Level Management	<p>4.2 Security of third-party access. Maintain the security of organizational information, processing facilities, and information assets accessed by third parties.</p> <p>4.3 Outsourcing. Maintain the security of information when the responsibility for information processing has been outsourced to another organization.</p> <p>6.1 Security in job definition and resourcing. Reduce the risks of human error, theft, fraud, or misuse of facilities.</p> <p>10.5 Security in development and support processes. Maintain the security of application system software and information; strictly control project and support environments.</p>	<p>1.1 Service Level Agreement Framework. Define a framework for service level agreements and the minimal contents.</p> <p>1.2 Aspects of Service Level Agreements. Reach agreement about the considerations that a service level agreement should address.</p> <p>1.3 Performance Procedures. Ensure that the manner of and responsibilities for performance governing relations (for example, non-disclosure agreements) between all the involved parties are established, coordinated, maintained, and communicated to all affected departments.</p> <p>1.4 Monitoring and Reporting. Appoint a service level manager who is responsible for monitoring and reporting on the achievement of the specified service performance criteria and all problems encountered during processing. The monitoring statistics should be analyzed on a timely basis.</p>

ITIL Discipline	ISO 17799 Controls	COBIT Controls
		<p>1.5 Review of Service Level Agreements and Contracts. Implement a regular review process for service level agreements and underpinning contracts with third-party service providers.</p> <p>1.6 Chargeable Items. Include provisions for chargeable items in the service level agreements to make trade-offs possible on service levels versus costs.</p> <p>1.7 Service Improvement Program. Implement a process to ensure that users and service level managers regularly agree on a service improvement program for pursuing cost-justified improvements to the service level.</p> <p>4.1 Operational Requirements and Service Levels. The system development life cycle methodology should ensure the timely definition of operational requirements and service levels.</p>
Capacity Management	<p>8.2.1 Capacity Planning. Capacity demands should be monitored and projections of future capacity requirements made to ensure that adequate processing power and storage are available.</p>	<p>3.7 Capacity Management of Resources. Establish a planning process for the review of hardware performance and capacity; this process should ensure that cost-justifiable capacity always exists to process the agreed workloads as well as provide the required performance quality and quantity prescribed in service level agreements.</p>
Continuity Management, Disaster Recovery, Business Continuity	<p>7.1 Secure areas. Prevent unauthorized access, damage, and interference to business premises and information by housing critical or sensitive business information processing facilities in secure areas, protected by a defined security perimeter, with appropriate security barriers and entry controls.</p> <p>7.2 Equipment security. Physically protect equipment from security threats and environmental hazards to prevent loss, damage, or compromise of assets and interruption to business activities.</p> <p>8.4.1 Information backup. Make backup copies of essential business information and software regularly.</p>	<p>4.3 IT Continuity Plan Contents. Ensure that a written plan is developed containing details for the continuity plan; emergency procedures; response procedures; coordination procedures; reconstruction procedures; communication procedures; and critical information on continuity teams, affected staff, customers, suppliers, public authorities, and media</p> <p>4.6 Testing the IT Continuity Plan. Assess the IT continuity plan adequacy on a regular basis and upon major changes to the business or IT infrastructure.</p>

ITIL Discipline	ISO 17799 Controls	COBIT Controls
	<p>11.1 Aspects of business continuity management. Counteract interruptions to business activities and protect critical business processes from the effects of major failures or disasters.</p> <p>12.1 Compliance with legal requirements. Avoid breaches of any criminal and civil law; statutory, regulatory, or contractual obligations; and of any security requirements by good design, operation, use, and management of information systems.</p>	<p>4.9 User Department Alternative Processing Back-up Procedures. Ensure that user departments establish alternative processing procedures that may be used until the IT function is able to fully restore its services after a disaster or an event.</p> <p>4.12 Off-site Back-up Storage. Establish off-site storage of critical back-up media, documentation, and other IT resources to support recovery and business continuity plans.</p> <p>11.23 Back-up and Restoration. Implement a proper strategy for back-up and restoration to ensure that it includes a review of business requirements as well as the development, implementation, testing, and documentation of the recovery plan.</p> <p>11.24 Back-up Jobs. Ensure that back ups are taken in accordance with the defined backup strategy and the usability of back ups is regularly verified.</p> <p>11.25 Back-up Storage. Include the proper storage of the data files, software, and related documentation—both on-site and off-site—in recovery plans.</p>
Availability Management	<p>6.3 Responding to security incidents and malfunctions. Minimize the damage from security incidents and malfunctions, and monitor and learn from such incidents.</p> <p>8.1 Operational procedures and responsibilities. Ensure the correct and secure operation of information processing facilities.</p> <p>8.5.1 Network controls. Implement a range of controls to achieve and maintain security in computer networks.</p> <p>11.1.2 Business continuity and impact analysis. Identify events (equipment failure, flood, fire, and so on) that can cause interruptions to business processes, then perform a risk assessment to determine the impact of those interruptions (both in terms of damage scale and recovery period).</p>	<p>4.2 IT Continuity Plan, Strategy, and Philosophy. Ensure that the IT continuity plan is in line with the overall business continuity plan to ensure consistency.</p> <p>4.4 Minimizing IT Continuity Requirements. Establish procedures and guidelines for minimizing the continuity requirements with regard to personnel, facilities, hardware, software, equipment, forms, supplies, and furniture.</p> <p>4.10 Critical IT Resources. Identify the critical application programs, third-party services, OSs, personnel, supplies, data files, and time frames needed for recovery after a disaster occurs.</p> <p>1.5 Review of Service Level Agreements and Contracts. Implement a regular review process for service level agreements and underpinning contracts with third-party service providers.</p>

ITIL Discipline	ISO 17799 Controls	COBIT Controls
		<p>10.1 Problem Management System. IT management should define and implement a problem management system to ensure that all operational events that are not part of the standard operation (incidents, problems and errors) are recorded, analyzed, and resolved in a timely manner.</p> <p>10.2 Problem Escalation. Define and implement problem escalation procedures to ensure that identified problems are solved in the most efficient way on a timely basis.</p> <p>12.6 Uninterruptible Power Supply. Management should assess regularly the need for uninterruptible power supply batteries and generators for critical IT applications to secure against power failures and fluctuations.</p>
IT Financial Management	<p>9.4.6 Segregation in networks. Divide large networks into separate logical network domains (such as an organization's internal network domains and external network domains), each protected by a defined security perimeter.</p> <p>2.3 Risk management. Identify, control, and minimize or eliminate security risks that may affect information systems, for an acceptable cost.</p>	<p>6.2 Costing Procedures. Define and implement costing procedures to provide management information about the costs of delivering information services while ensuring cost effectiveness.</p> <p>6.3 User Billing and Charge back Procedures. Define and use billing and charge back procedures that encourage the proper usage of computer resources and assure the fair treatment of user departments and their needs.</p> <p>1.9 Cost-Effective Security Controls. Ensure that the costs and benefits of security are carefully examined in monetary and non-monetary terms to guarantee the costs of controls do not exceed benefits.</p>